Regents Park Community College

ICT & Online Safety Policy

Policy updated: December 2023

Policy to be reviewed: December 2024

Non-Statutory

Contents

Key Details

Designated Safeguarding Lead(s): C Amos
Named Governor with lead responsibility: I Fielder
Online Safety Lead: N Moussa

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure.

Policy Rationale & Introduction

Rationale

This policy is set out in three sections in order to cover the main areas where information technology is prevalent in school. These are:

- The ICT curriculum
- The delivery of online safety guidance through the PSHE curriculum and the values programme
- Guidance for staff and students and parents

It outlines the range of the schools' technology systems and what is deemed as acceptable usage of these systems. These technologies encourage the development of communication skills and transform the learning process for all. This policy sets out the expectations of staff, students and other users (working for or on behalf of Regents Park Community College).

This policy is designed to express Regents Park Community College's philosophy with regard to the Internet, Intranet and electronic communication and general principles users should apply when using these services at the school site, when working from remote locations, when using the schools' name or when using resources provided by the school. This guidance does not attempt to cover every possible situation.

If a user is in doubt of whether an action may contravene policy then they should raise the concern with a member of staff listed on the key contacts page.

Introduction

The school believes that the creation of a safe ICT learning environment includes three main elements at the school:

An effective range of technological tools;

Policies and procedures, with clear roles and responsibilities;

Access to online safety information for students, staff, parents, carers and other users.

2. ICT Policy Aims

ICT is an integral part of the way our school works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under:

For staff - https://www.regentsparkcollege.org.uk/assets/Staff-Disciplinary-Policy-Procedures.pdf
https://www.regentsparkcollege.org.uk/assets/Code-of-Conduct.pdf

For students -
https://www.regentsparkcollege.org.uk/assets/Documents/Attachments/Behaviour-Policy-and-Procedures.pdf

2.1 Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

Data Protection Act 2018
The General Data Protection Regulation
Computer Misuse Act 1990
Human Rights Act 1998
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Education Act 2011
Freedom of Information Act 2000
The Education and Inspections Act 2006
Keeping Children Safe in Education
Searching, screening and confiscation: advice for schools

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the school to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors

“Personal use”: any use or activity not directly related to the users’ employment, study or purpose

“Authorised personnel”: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

“Materials”: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school’s ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

- Unacceptable use of the school’s ICT facilities includes:
- Using the school’s ICT facilities to breach intellectual property rights or copyright
- Using the school’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school’s policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school’s ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school’s filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher and/or Network Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school’s ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

- Contact the Network Manager to discuss restrictions
- Formally write to the Headteacher to explain your needs

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on:

For staff - https://www.regentsparkcollege.org.uk/assets/Staff-Disciplinary-Policy-Procedures.pdf
https://www.regentsparkcollege.org.uk/assets/Code-of-Conduct.pdf

For students -
https://www.regentsparkcollege.org.uk/assets/Documents/Attachments/Behaviour-Policy-and-Procedures.pdf

Students will receive an automatic week ban and a phone call home for breaching the web filtering policy.
Students will receive a 1 week ban from the all IT systems and a phone call home for all forms of misuse, this can be extended by the Network Manager / HOY / LT.

https://www.regentsparkcollege.org.uk/assets/Documents/Attachments/Behaviour-Policy-and-Procedures.pdf

https://www.regentsparkcollege.org.uk/assets/Staff-Disciplinary-Policy-Procedures.pdf

https://www.regentsparkcollege.org.uk/assets/Code-of-Conduct.pdf

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files
- Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.
- Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network Manager
- Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Network Manager and/or LT may withdraw permission for it at any time or restrict access at their discretion.
- Personal use is permitted provided that such use:
- Does not take place during contracted hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes
- Staff may not use the school's ICT facilities to store personal non-work-related

information or materials (such as music, videos, or photos).

- Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
- Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parents could see them.
- Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2 Staff use of devices for both personal and work use

Expectations

- Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.3 Officially provided mobile phones and devices

Members of staff will be issued with a work phone number and email address, where contact with students or parents/ carers is required. Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff. They must always be used in accordance with the acceptable use policy and other relevant policies.

5.4 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers. Unless permission is sought with exceptional circumstances and the staff number hidden.
- Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) and/or Headteacher.
- Staff will not use personal devices:
- To take photos or videos of students and will only use work-provided equipment for this purpose.

- Directly with students and will only use work-provided equipment during lessons or educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

5.5 Staff use of email for both personal and work

The school provides each member of staff with an email address. This mail account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.

- Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error which contains the personal information of another person, they must inform the Network Manager and Data Protection Officer immediately and follow our data breach procedure.
- The use of personal email addresses by staff for any official setting business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents.
- Communication to parents is sent via our generic email address info@regentspark.southampton.sch.uk

5.6 Personal social media accounts

The purpose of this policy is to set out the school's recommendations and requirements for the use of social networking media by its employees. In doing so, the school seeks to achieve an appropriate balance in the use of social networks by staff as private individuals, but also as employees and educators, with professional reputations and careers to maintain, and contractual and legislative requirements to adhere to.

- Whilst the school does not wish to discourage staff from using such sites on the

Internet in their personal time, it does expect certain standards of conduct to be observed in order to protect the school and its reputation, and also to protect staff from the dangers of inappropriate use.

- Accessing social networking sites in working time and/or from school ICT equipment is strictly forbidden, whether the equipment is used at home or at school.
- Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.
- The school has guidelines for staff on appropriate security settings for Facebook accounts
  (see appendix 1).
- Please refer to the school's social networking policy for full details.

Communicating with students and parents and carers

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Headteacher (see Staff Code of Conduct for further information). If ongoing contact with students is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.

Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher/manager. Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputies).

5.7 School Official social media accounts and use

Regents Park Community College official social media channels are a Twitter, Instagram and Facebook account: @RegentsParkCC. These are managed by the Business Manager and Deputy Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
- Admin staff have access to account information and login details for our social

media channels, in case of emergency, such as staff absence

- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff use setting provided email addresses to register for and manage any official social media channels.
- Official social media sites are suitably protected and linked to our website.
- Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti- bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving students will be moderated if possible.
- Parents and carers will be informed of any official social media use with students; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our acceptable use policy.
- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role but make it clear that they do not necessarily speak on behalf of the setting.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current students.
- Inform their line manager, the DSL (or deputies) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from students.

5.8 Social Media
Expectations

The expectations' regarding safe and responsible use of social media applies to all members
of Regents Park Community College. All members of Regents Park Community College are expected to engage in social media in a positive, safe and responsible manner. We will control student and staff access to social media whilst using setting provided devices and systems on site.

Concerns regarding the online conduct of any member of Regents Park Community College community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

5.9 Remote access

We allow some staff to access the school's ICT facilities and materials remotely.

The school uses TeamViewer and Tile Academy to allow LT and core staff to access the school's systems remotely. TeamViewer and Tile Academy are managed by the IT Services team and available so that core staff can access systems such as but not limited to:

Active Directory
Sims.Net
Personnel systems
SBS
Unit4 Business World
SCC Portal
Mapped Network Drives

TeamViewer is a licenced product and the free version should not be used as an alternative, please contact both the Network Manager and Headteacher if you require access making your need of use clear in writing.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Network Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.
https://www.regentsparkcollege.org.uk/assets/Documents/Attachments/Data-Protection-Policy.pdf

5.10 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network.
This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls

- User activity/access logs
- Any other electronic communications

Only authorised IT Services staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5.11 Staff Misuse

Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy.

For any allegations regarding a member of staff's online conduct a consultation will be sort with the LADO (Local Authority Designated Officer). Appropriate action will be taken in accordance with our staff code of conduct/teaching standards.

6. Students

6.1 Access to ICT facilities

"Computers and equipment in the school's ICT suite are available to students only under the supervision of staff"

"Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff"

"Students will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL http://classroom.google.com

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the behaviour, if a student engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- See section 4.2 for a list of possible sanctions.

6.4 Students' Use of Personal Devices and Mobile Phones

Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

- Regents Park Community College expects students' personal devices and mobile phones to be switched off and out of sight during the school day.
- If a student needs to contact his/her parents or carers they will be allowed to use a setting phone or staff will make the call on their behalf.
- Parents are advised to contact their child via the setting office.
- Mobile phones or personal devices will not be used by students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
- Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a student breaches the policy, the phone or device will be confiscated and will be held in a secure place.
- Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with our policy. https://www.gov.uk/government/publications/searching-screening-and-confiscation
- Students` mobile phones or devices may be searched by a member of the leadership team, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.

https://www.gov.uk/government/publications/searching-screening-and-confiscation)

- Mobile phones and devices that have been confiscated will be released to parents or carers.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

6.5 Students' Personal Use of Social Media & Gaming Sites

Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources. Advice is given during ICT lessons on online safety.

We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for students under this age.

Any concerns regarding students use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.

Students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.
- To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

6.6 Student email

Students will be provided with a Google Classroom email accounts for educational purposes.

Students will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

6.7 Student internet access

The school provides students with access to the internet using any school owned device. All students have the same level of filtering unless their teacher has gained permission for them to view additional web content.

Students are not permitted to use their personal devices on the school's network for security reasons

7. Parents/Visitors

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in Appendix 2.

7.3 Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use. Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Headteacher of any breaches our policy.

7.4 Internet access

Parents and visitors to the school will not be permitted to use the school's internet connection unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's internet connection in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Staff must not allow anyone who is not authorised to have access to the school's internet connection. Doing so could result in disciplinary action.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

All students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system. (upper and lowercase, numbers and special characters)
- Change their passwords twice a year
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.
- 2 Factor Authentication

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti- virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.
https://www.regentsparkcollege.org.uk/assets/Documents/Attachments/Data-Protection-Policy.pdf

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the IT Services Team.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user

should not have access to is shared with them, they should alert the Network Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption. School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager.

9. Internet access

The school's internet connection is secured.

The school operates a Smoothwall UTM (Unified Treat Management) appliance. This appliance acts as both a firewall and web filter for all inbound and outbound internet traffic.

The Smoothwall web filter is separated into a series of user policies. This allows staff and students to have different levels of filtering and also allow small groups to have temporary access to usually blocked material.

Web filters are not fool-proof so any inappropriate sites that the filter hasn't identified or appropriate sites that have been filtered in error should be reported to ictsupport@regentspark.southampton.sch.uk

10. Online Safety Policy & Aims

This online safety policy has been adapted involving staff, students and parents/carers.

It takes account of the DfE statutory guidance Keeping Children Safe in Education 2022 and the Southampton City Council Safeguarding Children Partnership procedures.

The purpose of this online safety policy is to:

- Safeguard and protect all members of our community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

We identify that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

11. Policy Scope

We believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.

We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

We believe that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as students, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school but is linked to member of the school.

In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school.

12. Roles and Responsibilities

The Online Safety Lead (OSL) is responsible for online safety, however ultimately the Designated Safeguarding Lead (DSL) M Webster, Deputy Headteacher has lead responsibility for safeguarding concerns and online safety. Network Manager also has a lead role in ensuring the online safety of the school community.

Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL. We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

12.1 The leadership and management team and governors will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running interrelated theme whilst devising appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that they are doing all that they reasonably can to limit children's exposures

to risks from the school's IT system and therefore have suitable and appropriate filtering and monitoring systems are in place. They will have an awareness and understanding of the provisions in place and will work with technical staff to monitor the safety and security of our systems and networks.

- Ensure that they regularly review the effectiveness of filters and monitoring systems; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- Recognise that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice, ideally annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.
- Communicate with parents regarding the importance of children being safe online, the systems being used in school and information regarding what their children are being asked to do online by the school.

12.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Liaise with staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote

positive online behaviour, such as Safer Internet Day.

- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings
- safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns to the SLT.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly termly with the governor with a lead responsibility for safeguarding and online safety.
- The triangulation meeting will also consider patterns of online safety issues to support the
- DSL and to work with the IT and RSHE leads to address issues in the curriculum.

12.3 It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Reinforce the school's online safety messages when teaching lessons online

12.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially

in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised. This includes using 2 factor authentication where available, unique passwords, not allowing users to re-use passwords and changing passwords frequently. Our additional security measures include; web filtering, spam filtering, network firewall, anti-virus, end point encryption and ransomware protection and online back ups.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

12.5 It is the responsibility of students (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to Acceptable Use Policies.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

12.6 It is the responsibility of parents and carers to:

- Read the Acceptable Use Policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the Acceptable Use Policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

13. Education and Engagement Approaches

13.1 Education and engagement with students

We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst students by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety through IT lessons and Cyber Ambassadors.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Regents Park Community College will support students to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.

13.2 Vulnerable Students

Regents Park Community College recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content or behaviours without understanding the consequences of doing so.

Regents Park Community College will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

When implementing an appropriate online safety policy and curriculum Regents Park Community College will seek input from specialist staff as appropriate, including the SENCO, Designated Teacher for LAC and other appropriate staff.

13.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be done through stand-alone sessions or through drip feeding with small sessions/ daily bulletin reminders. We have also purchased some online training to support staff.
- This will cover the potential risks posed to students (Content, Contact, Conduct and

Commerce) as well as our professional practice expectations. (NM/PW)
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

13.4 Awareness and engagement with parents and carers

We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and transition events.
- Drawing their attention to the online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information as part of joining our community.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

14. Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content.

All members of the community will be directed to the DSL or Headteacher in such circumstances.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. We require staff, parents, carers and students to work in partnership to resolve online safety issues.

After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice Southampton City Council's Safeguarding Team.

Where there is suspicion that illegal activity has occurred contact the Hampshire Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other

local settings are involved or the public may be at risk), the DSL or Headteacher will contact Hampshire Police first to ensure that potential investigations are not compromised.

14.1 Concerns about Students' Welfare

The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL (or deputies) will record these issues in line with our child protection policy.

The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Southampton Safeguarding Children Partnership thresholds and procedures.

We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

15 Procedures for Responding to Specific Online Incidents or Concerns

15.1 Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood part 5 of Keeping Children Safe in Education.

We recognise that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include; non-consensual sharing of nudes and semi-nudes images and videos, sharing of unwanted explicit content, upskirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children. We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- If content is contained on students electronic devices, they will be managed in accordance with the DfE ' searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour for learning policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with Hampshire Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

15.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')

We recognise youth produced sexual imagery (known as "sharing nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will:

- follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people
- ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability appropriate educational methods. For example, sharing information from National Online Safety.
- ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.– **in most cases, images or videos should not be viewed**
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policy.
- Ensure the DSL (or deputy) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
- Store the device securely. If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Care and/or the Police, as appropriate.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

15.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)

- We will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to students and other members of our community. This is on our website. If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation)

  We will:
- Act in accordance with our child protection policies and the relevant Hampshire & IOW Safeguarding Child Partnership's procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)

- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If students at other settings are believed to have been targeted, the DSL (or deputy) will contact the Police.

15.4 Indecent Images of Children (IIOC)

We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet service provider (ISP) which implements appropriate filtering, firewalls and anti-spam software.
If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Hampshire or the LADO.

If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy DSL) is informed, who will investigate the incident.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy DSL) and Headteacher are informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

- Ensure that any copies that exist of the image, for example in emails, are deleted once directed to by the police.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

15.5 Cyberbullying

All staff will understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated here. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

15.6 Cybercrime

We will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme. We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

15.7 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at our setting and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Hampshire Police.

15.8 Online Radicalisation and Extremism

Regents Park Community College will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation.

We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site. Internet use is monitored through the Smoothwall systems with daily reporting of risk categories to the safeguarding team.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.

If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

16. Safer Use of Technology

16.1 Classroom Use

Regents Park Community College uses a wide range of technology.
This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and students complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their ability and understanding.

16.2 Managing Internet Access

We will maintain a written record of users who are granted access to our devices and systems.
All staff, students and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

16.3 Filtering and Monitoring

16.3.1 Decision Making

Regents Park Community College governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit student's exposure to online risks.

- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the

filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

16.3.2 Filtering

- Education broadband connectivity is provided through BT.
- We use Smoothwall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with BT and Smoothwall to ensure that our filtering policy is continually reviewed.

If students discover unsuitable sites, they will be required to:

- **Turn off monitor/screen and report the concern immediate to a member of staff.**
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Hampshire Police or CEOP.

16.3.3 Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- Use of our monitoring systems such as Smoothwall. Reports are sent to the Business Manager and Headteacher to investigate
- If a concern is identified via monitoring approaches we will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

16.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

16.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

16.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or student's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

16.7 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

16.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email i.e. AnyComms.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community should inform the Lead DSL or a deputy DSL if they receive offensive communication, and this will be actioned and recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted;
- access to external personal email accounts should not be used during the school day.
- We have a dedicated link on our school website whereby students can report when they have a safeguarding concern including online abuse in addition to CEOPs link. www.regentsparkcollege.org.uk/home/parents/safeguarding

16.9 Remote Learning

At Regents Park Community College, we understand the need to continually deliver high quality education, including during periods of remote working – whether for an individual student or multiple. We recognise the importance of maintaining high expectations in all areas of school life and ensuring that all students have access to the learning resources and support they need to succeed.

Through the implementation of our remote learning procedure, we aim to address the key concerns associated with remote working, such as online safety, access to educational resources, data protection, and safeguarding.

For more details, please refer to our remote learning procedure.

16.10 Management of Google Classroom

- Leaders and staff will regularly monitor the usage of the Google Classroom (GC), including message/communication tools and publishing facilities.
- Only current members of staff, students and parents will have access to the GC. When staff and/or students leave the setting, their account will be disabled.
- Students and staff will be advised about acceptable conduct and use when using the GC.
- All users will be mindful of copyright and will only upload appropriate content onto the GC.
- Any concerns about content on the GC will be recorded and dealt with in the following ways:
- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator. Access to the GC for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement. A student's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

17.11 Management of Applications (apps) used to Record Children's Progress

We use SIMS to track student's progress and share appropriate information with parents and carers.

The Headteacher/manager is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard student's data:

- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store students' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

18. Use of Personal Devices and Mobile Phones

We recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

18.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- All members of Regents Park Community College are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of Regents Park Community College are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms and student toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of Regents Park Community College are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

19. Artificial Intelligence (AI)

Regents Park Community College is committed to harnessing the transformative capabilities of Artificial Intelligence (AI) to enrich the educational journey of its students. Through AI, we aim to offer personalised learning experiences, streamline administrative processes, and present innovative engagement methods for teachers. Concurrently, we acknowledge the ethical and safety considerations intrinsic to AI's application

19.1 Application of AI in Learning, Teaching & Assessment

While students are encouraged to utilise AI to bolster their learning, they must strictly adhere to guidelines set out below:

- Validating AI-suggested concepts against credible sources.
- Recognising AI's potential limitations, biases, and the risks of misinformation.
- Not presenting AI-generated content as their own original work.
- Appropriate referencing of AI-derived content, acknowledging that it won't be credited on its intrinsic merit.
- Detailed acknowledgment of AI tools utilised, ensuring the retention of evidence of their usage.

Regents Park Community College's teaching staff play a pivotal role in guiding and supervising the ethical use of AI in education.

Responsibilities encompass:

- Taking part in training on the advantages, risks, and ethical use of AI.
- Integrating AI understanding and application within the curriculum.
- Monitoring student submissions for possible AI misuse.

- Ensuring alignment with JCQ guidelines on AI's role in assessments.

19.2 Public Examinations & Non-Examined Assessment (NEA)
AI tools may be utilised during assessments under specific conditions, ensuring the work is a true reflection of a student's independent endeavours. Any misuse of AI, such as plagiarising or producing misleading references, will be treated seriously.

19.3 Ethical use of Artificial Intelligence
Upholding our commitment to ethical standards, we expect all AI users within Regents Park Community College to:

- Respect privacy and intellectual property rights.
- Refrain from actions that might result in discrimination or unjust outcomes.
- Adhere to all pertinent laws, regulations, and school policies, particularly concerning data privacy.
- Stay informed about potential AI biases and actively work to mitigate them.
- Abide by stringent data governance norms, ensuring adherence to GDPR and the school's
- Data Policies.

Consistent training sessions on AI's ethical, transparent, and safe use will be organised for both staff and students. Regular monitoring ensures AI systems' alignment with our ethical commitments.

20. Monitoring and review

Technology in this area evolves and changes rapidly, the Headteacher and Network Manager will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school including any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure

This policy will be reviewed every 3 years.

The Governing Body is responsible for approving this policy. The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

21. Related policies

This policy should be read alongside the school's policies on:
Safeguarding and child protection
Behaviour
Staff discipline
Data protection/GDPR
Code of conduct
Social media policy
Staff Mobile Phones
Anti-bullying policy
Remote Learning Policy

National Links and Resources for Educational Settings
CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk

Childnet: www.childnet.com
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: Net-Aware
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools: www.360safe.org.uk
Get Safe Online: www.getsafeonline.org
Action Fraud: www.actionfraud.police.uk
Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk)

National Links and Resources for Professionals/Parents/Carers

There is a wealth of information available to support schools and parents/carers to keep children safe online. See Keeping Children Safe in Education 2023 Part 2 for more resources.

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from students on social media

10 rules for school staff on Facebook

Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

Change your profile picture to something unidentifiable, or if not, ensure that the image is professional

Check your privacy settings regularly

Be careful about tagging other staff members in images or posts

Don't share anything publicly that you wouldn't be just as happy showing your students

Don't use social media sites during school hours

Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there

Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)

Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or students)

Check your privacy settings

 Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

 Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

 The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

 Google your name to see what information about you is visible to the public

 Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

 Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A student adds you on social media

 In the first instance, ignore and delete the request. Block the student from viewing your profile

 Check your privacy settings again, and consider changing your display name or profile picture

 If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages

 Notify the Senior Leadership Team or the Headteacher about what's happening

A parent adds you on social media

 It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

 If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

 Do not retaliate or respond in any way

 Save evidence of any abuse by taking screenshots and recording the time and date it occurred

 Report the material to Facebook or the relevant social network and ask them to remove it

 If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

 If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

 If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: Our official Facebook page Out official Twitter page Sims Parent App Email/text groups for parents (for school announcements and information) □ Our virtual learning platforms	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: Be respectful towards members of staff, and the school, at all times Be respectful of other parents/carers and children Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident □ Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older students

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers	
Name of student:	
When using the school's ICT facilities and accessing the internet in school, I will not: Use them for a non-educational purpose Use them without a teacher being present, or without a teacher's permission Use them to break school rules Access any inappropriate websites Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) Use chat rooms Open any attachments in emails, or follow any links in emails, without first checking with a teacher Use any inappropriate language when communicating online, including in emails Share my password with others or log in to the school's network using someone else's details Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger students

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers	
Name of student:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: Use them without asking a teacher first, or without a teacher in the room with me Use them to break school rules Go on any inappropriate websites Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) Use chat rooms Open any attachments in emails, or click any links in emails, without checking with a teacher first Use mean or rude language when talking to other people online or in emails Share my password with others or log in using someone else's name or password Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) Use them in any way which could harm the school's reputation Access social networking sites or chat rooms Use any improper language when communicating online, including in emails or other messaging services Install any unauthorised software, or connect unauthorised hardware or devices to the school's network Share my password with others or log in to the school's network using someone else's details Share confidential information about the school, its students or staff, or other members of the community Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6 – Software Catalog

Please be aware that Regents Park Community College can provide access to the software below. However, some of the packages may be limited in terms of which devices they can be installed on or indeed how many licences the school has for them. All requests for additional software should be emailed to itservices@regentspark.southampton.sch.uk.

If staff are at all unsure about the safety of a particular piece of software that they would like to install they should consult the IT Support Team.

Regents Park Licensed Software	Additional Open Source Software	Blacklisted Software (not to be used)
Microsoft Server 2008, 2012, 2016, 2019 Microsoft Windows 7, 10 Microsoft Office 2003, 2010, 2013, 2016, 2019 Capita Sims.Net Sims InTouch Sims Parent Sims Parents Evening (SchoolCloud) ShowMyHomework (Satchel1) GDPRiS Impero Console LiveDrive Promethean Activ Studio Promethean Activ Inspire Starboard 7.0 Genie Backup Manager Eclipse and MLS Connect Comic Life Lexia Reading LOGIT Lab 4 Lucid LASS Lucid Memory Booster Lucid Exact Techsoft 2D Design Techsoft 2D Design V2 Exam Wizard PE PCB Wizard Livewire Control Studio Papercut Serif Media Suite Visit-ED Tucasi Schools Cash Office	Google Chrome Google Apps Sync Google Drive Google Classroom Dropbox Free Studio Safari Quicktime ITunes VLC Player Picasa Movie Maker 7-Zip Daemon Tools Lite Astroburn Google Earth ICloud Screen-Cast-O-Matic Wink Hat Randomiser Microsoft Security Essentials Shrewsoft VPN Client Adobe Premiere Pro 2.0 Adobe Audition 3.0 Adobe Photoshop CS2 Fortinet VPN SSL Client Teamviewer Zoom Loom	Napster Morpheus UTorrent Any Peer-to-peer file sharing Any other virus protection

Lexia CPOMS SISRA Online SISRA Analytics Eclipse (Reading Cloud) Read Write Gold		

Appendix 7 - Email and Messaging – Good Practice Guide

Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment Formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
Email Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of Emails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own Email address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential Record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of Emails could be used in support, or in defence, of the Academy's legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the Email can result in legally binding contracts being put into place.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them.
Email threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is

	best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	Email in the right context, care should be taken to use Email where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
Forwarding Emails	Consideration should be given when forwarding Emails that it may contain information that you should consult with the originator before passing to someone else.

RPCC Mobile Phone Disclaimer

In order to support staff members, Regents Park supply teaching staff with a school mobile phone to make external calls to parents.

I confirm that I do/do not require a mobile phone for this purpose.

I accept all responsibility for the use of my personal mobile phone and any costs incurred.

I accept all responsibility for the use and condition of my work mobile phone ensuring it is kept locked when not in use.

I confirm that I will ensure that my phone number will be withheld before contacting parents.

I am aware that there are various landlines around the school that I can use instead of using a mobile phone.

Name:……..

Staff Signature:…… Dated:……

Business Manager Signature:…… Dated:……