HILLVIEW
SCHOOL FOR GIRLS

ICT POLICY

INCLUDING CANTEEN, COPYING SYSTEMS *AND* CCTV

CONTENTS PAGE

INTRODUCTION

1. All Hillview School for Girls (Hillview) information communication technology (ICT) facilities and information resources remain the property of Hillview and not of particular individuals, teams or departments. By following this policy, we will help ensure that ICT facilities are used:

- legally;
- securely;
- without undermining Hillview;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so that they remain available.

2. The policy relates to all ICT facilities and services provided by Hillview, although special emphasis is placed on email and the internet. All employees and any other users of our IT are expected to adhere to the policy.

3. Use of the Internet by employees is permitted and encouraged where such use supports the goals and objectives of Hillview.

4. Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from Hillview's IT equipment. Remote Access is available to all employees.

5. Hillview uses closed circuit television (CCTV) images to reduce crime and monitor Hillview buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property, comprising a number of fixed and dome cameras without sound recording capability.

6. Hillview complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

7. Hillview's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The use of CCTV, and the associated images and any sound recordings is covered by the Data Protection Act 2018. This policy outlines Hillview's use of CCTV and how it complies with the Act.

Disciplinary Measures

1. Deliberate and serious breach of the policy statements in this section may lead to Hillview taking disciplinary measures in accordance with the Hillview Fairness at Work Policy. Hillview accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employees' productivity and the reputation of the organisation.

2. In addition, all of the organisation's phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

APPENDIX 1

SECURITY

1. As a user of Hillview's equipment and services, you are responsible for your activity.

2. Do not disclose personal system passwords or other security details to other employees, or external agents, and do not use anyone else's log-in; this compromises the security of Hillview. If someone else gets to know your password, ensure that you change it or get ICT Technical Support to help you.

3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where members of the public have access to the screen in your absence.

4. Any pen drives or other storage devices used on Hillview's network should be secure and only those that are the property of Hillview should be used. Please see Appendix, Removable Data for more detail.

5. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact ICT Technical Support.

APPENDIX 2

USE OF EMAIL

1. When to use email:
   (a) Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

   (b) Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees of Hillview is permitted and encouraged where such use supports the goals and objectives of Hillview.

2. However, Hillview has a policy for the use of email whereby employees must ensure that they:
   - comply with current legislation;
   - use email in an acceptable way;
   - do not create unnecessary business risk to Hillview by their misuse of the internet.

Unacceptable Behaviour

(a) Sending confidential information to external locations without appropriate safeguards in place. See Appendix 3, Confidentiality, point 2 of this document for more details.

(b) Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

(c) Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

(d) Using copyrighted information in a way that violates the copyright.

(e) Breaking into Hillview's or another organisation's system, or unauthorised use of a password / mailbox.

(f) Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

(g) Transmitting unsolicited commercial or advertising material.

(h) Undertaking deliberate activities that waste employee's effort or networked resources.

(i) Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

Confidentiality

Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. Hillview reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users within and outside the system as well as deleted messages. See Appendix 3, Confidentiality, point 2 for more detail.

General points on email use

(a) When publishing or transmitting information externally be aware that you are representing Hillview and could be seen as speaking on Hillview's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

(b) Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

(c) Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary;

(d) Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague);

(e) Do not forward emails warning about viruses (they are invariably hoaxes and ICT Technical Support will probably already be aware of genuine viruses – if in doubt, contact them for advice);

(f) Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open **report.doc** from a colleague you know but do not open **explore.zip** sent from an address you have never heard of, however tempting. Alert ICT Technical Support if you are sent anything like this unexpectedly; this is one of the most effective means of HILLVIEW against email virus attacks.

Email signatures

Keep these short and include your name, title, phone numberand website address.

APPENDIX 3

USE OF THE INTERNET

Employees must ensure that they:

(a) comply with current legislation;

(b) use the internet in an acceptable way;

(c) do not create unnecessary business risk to the organisation by their misuse of the internet.

Unacceptable Behaviour

In particular, the following is deemed unacceptable use or behaviour by employees (this list is non-exhaustive):

(a) Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

(b) Using the computer to perpetrate any form of fraud, or software, film or music piracy;

(c) Using the internet to send offensive or harassing material to other users;

(d) Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

(e) Hacking into unauthorised areas;

(f) Creating or transmitting defamatory material;

(g) Undertaking deliberate activities that waste employee's effort or networked resources;

(h) Deliberately or recklessly introducing any form of computer virus into Hillview's network.

Chat Rooms/Instant Messaging (IM)

The use of chat rooms and instant messaging is permitted for business use only.

Webmail

The use of webmail (e.g. Hotmail, MSN, Google Mail) is not permitted in the organisation unless previously agreed with ICT Technical Support.

Obscenities / Pornography

Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

Copyright

1. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

2. Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

Confidentiality

1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

2. If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the Director of Finance & Administration (DFA).

    (a) Personal, sensitive and / or confidential information should be contained in an attachment;
    (b) In appropriate cases the attachment should be encrypted, and / or password protected;
    (c) Any password or key must be sent separately;
    (d) Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;
    (e) Do not refer to the information in the subject of the email.

APPENDIX 4

HILLVIEW'S NETWORK

1. Keep master copies of important data on Hillview's network server and not solely on your PC's local C: Drive or portable disks. Not storing data on Hillview's network server means it will not be backed up and is therefore at risk.

2. Ask for advice from ICT Technical Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

3. Be considerate about storing personal (non-Hillview) files on Hillview's network.

4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

Removable media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must first contact the DFA for permission, but

I. Always consider if an alternative solution already exists;
II. Only use recommended removable media;
III. Encrypt and password protect;
IV. Store all removable media securely;
V. Removable media must be disposed of securely by ICT Technical Support.

Personal use of ICT Facilities

Social Media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

Use of Social Media at work

1. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities. Access to particular social media websites may be withdrawn in the case of misuse.

2. Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee. It is, therefore, imperative that you are respectful of the organisation's service as a whole including clients, colleagues, partners and competitors.

3. Employees should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of Hillview unless appropriately authorised to do so. Personal opinions must be acknowledged as such and should not be represented in any way that might make them appear to be those of the organisation. Where appropriate, an explicit disclaimer should be included.

4. Any communications that employees make in a personal capacity must not:

(a) bring Hillview into disrepute, for example by criticising clients, colleagues or partner organisations;
(b) breach the Hillview's policy on client confidentiality or any other relevant policy;
(c) breach copyright, for example by using someone else's images or written content without permission;
(d) do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;
(e) use social media to bully another individual;
(f) post images that are discriminatory or offensive (or links to such content).

5. Hillview maintains the right to monitor usage where there is suspicion of improper use.

Other Personal Use

1. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

(a) incur specific expenditure for Hillview;
(b) impact on the performance of your job or role (this is a matter between each employee and their line manager);

(c) break the law;
(d) bring Hillview into disrepute;
(e) detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);
(f) impact on the availability of resources needed (physical or network) for business use.

2. Any information contained within Hillview in any form is for use by the employee for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of the Business Manager.

APPENDIX 5

PERSONAL PORTABLE AND MOBILE ICT EQUIPMENT

1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to Appendix 4, Removable Media of this document when considering storing or transferring personal or sensitive data.

(a) Use of any portable and mobile ICT equipment must be authorised by ICT Technical Support before use.

(b) All activities carried out on Hillview's systems and hardware will be monitored in accordance with the general policy.

(c) Employees must ensure that all data belonging to Hillview is stored on Hillview's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

(d) Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

(e) Synchronise all locally stored data, including diary entries, with the central organisation network server on a frequent basis.

(f) Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

(g) The installation of any applications or software packages must be authorised by the DFA, fully licensed and only carried out by ICT Technical Support.

(h) In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

2. Portable equipment must be transported in a protective case if one is supplied.

Remote Access

1. You are responsible for all activity via your remote access facility.

2. Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

3. To prevent unauthorised access to Hillview's systems, keep all remote access information such as, logon IDs, passwords and PINs confidential and do not disclose them to anyone.

4. Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

5. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

6. Protect Hillview's information and data at all times, including any printed material produced while using the remote access facility.

7. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

8. Care should be taken when working on laptops in public places (e.g. trains) that any employee or client details are not visible to other people.

Electronic Monitoring

1. You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

(a) In the case of a specific allegation of misconduct, when the Human Resources Manager (HRM) can authorise accessing of such information when investigating the allegation;

(b) When ICT Technical Support cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

Online Purchasing

Any users who place and pay for orders online using personal details do so at their own risk and Hillview accepts no liability if details are fraudulently obtained whilst the user is using Hillview's equipment.

Care of Equipment

Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting ICT Technical Support.

Agreement

All employees, who have been granted the right to use the Hillview's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signed:		**Signed:**	
Manager:		**Employee:**	
Date:		**Date:**	

APPENDIX 6

CATERING AND COPYING SYSTEMS

The school uses a fob system for the use of the canteen and photocopying facilities. This enables staff and students to access the facilities and to keep track of their expenditure.

In both cases, the personal information is held in the school's management information system and the programmes used in the canteen and copying systems only use the information they need to identify the member of staff or the student. This is usually a roll number or other unique identifying reference. The canteen and copying systems have no access to any personal details. In the case of the canteen, the service is provided by Independent Catering Limited and the till system is operated by Cunninghams Limited. The till system only holds the student admission number and their date of birth as a reference. Neither company has any access to any other personal information. The copying system is provided by Ricoh Limited and the copy access system is provided by Papercut Limited. Neither company has any access to any personal information.

There is no personal information contained on the fob itself. This means that in the event of the fob being lost, there is no risk of any personal data being lost.

APPENDIX 7

CCTV

1. The CCTV system is owned and operated by Hillview, the deployment of which is determined by Hillview's leadership team and is monitored centrally from Hillview offices.

2. The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and Hillview community.

3. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by Hillview data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

4. CCTV warning signs will be clearly and prominently placed at all external entrances to Hillview, including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see appendix B). In areas where CCTV is used, Hillview will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

5. The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Siting the Cameras

1. Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. Hillview will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act 2018.

2. Hillview will make every effort to position cameras so that their coverage is restricted to Hillview premises, which may include outdoor areas.

3. CCTV will not be used in classrooms but in areas within school that have been identified by staff and pupils as not being easily monitored.

4. Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

1. Hillview may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

2. In these circumstances authorisation must be obtained from a member of the senior leadership team.

3. Covert monitoring must cease following completion of an investigation.

4. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

Storage and Retention of CCTV images

1. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

2. All retained data will be stored securely.

Access to CCTV images

Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

Subject Access Requests (SAR)

1. Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act 2018.

2. All requests should be made in writing to the Business Manager (SBM). Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

3. Hillview reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Access to and Disclosure of Images to Third Parties

1. There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to Hillview where these would reasonably need access to the data (e.g. investigators).

2. Requests should be made in writing to the Headteacher.

3. The data may be used within Hillview's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Complaints and enquiries about the operation of CCTV within Hillview should be directed to the SBM in the first instance.

Further Information

Further information on CCTV and its use is available from the following:

- Surveillance Camera Code of Practice (Updated 2022)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018

It is a requirement of the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. Hillview is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- **That the area is covered by CCTV surveillance and pictures are recorded**
- The purpose of using CCTV
- The name of Hillview
- The contact telephone number or address for enquiries

Hillview School for Girls
Trustees' ICT Policy, including Canteen, Copying & CCTV

Main compilers: Alison Newman, Business Manager

Most recent update: June 2022

Date of approval by trustees: 16 June 2022

Consulted: Students Reports & Records;

- Surveillance Camera Code of Practice (Updated 2022)

Data Protection Act 2018

Anticipated Review date: June 2024