Policy Document

Cottenham Village College

E-Safety

Associated policies:
Acceptable Use Policy for students
Acceptable Use Policy for parents/ carers
Acceptable Use Policy for Staff
Safeguarding policy
Behaviour Policy

General policy statement
Cottenham Village College will endeavour to ensure the e-safety of the school community. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

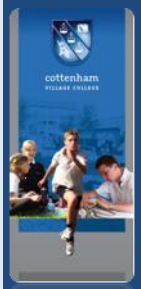
Cottenham Village College is committed to ensuring that students are educated about the benefits and risks of using new technologies both inside and outside of the school environment. Safeguards, rules and expectations will guide both staff and students in safer use of such technologies and in their on-line experiences.

Cottenham Village College will ensure that there is adequate training for staff and volunteers.

Rationale
The purpose of this policy is to:
- set out the key principles expected of all members of the school community at Cottenham Village College with respect to the use of IT-based technologies;
- safeguard and protect the children and staff of Cottenham Village College;
- assist school staff to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use;
- have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies;
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

This policy applies to:
- Students
- All teaching and support staff, including volunteers
- Members, trustees and governors

Communication:
The policy will be communicated to staff/students/ parents/carers in the following ways:
- Policy will be posted on the school website / staffroom notice board
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with students at the start of each year.
- AUP and safer use of Internet will be covered in depth with students as they enter the school in Year 7.
- AUP detailed agreement is in each student's planner. Students and parents/carers will sign this agreement



What is E-Safety?
Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Children and young people need the help and support of the College to recognise and avoid e-safety risks and to build their resilience.
Some examples of such risks are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Exposure to external and inappropriate influences (radicalisation)
- Physical danger of sexual abuse
- Grooming

At the College, it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together. The purpose of this e-safety policy is to outline what measures the College takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

The College Trust's E-safety policy will work alongside other relevant policies such as:

- Acceptable Use Policies (students, parents, staff)
- Safeguarding Policy (including the Prevent Duty Statement)
- Behaviour Policy (including bullying)

Cottenham Village College's E-safety policy has been developed by the College E-safety Committee. This working group consists of:

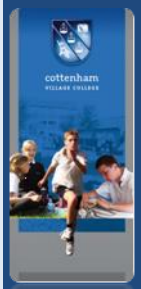
- Deputy Headteacher i/c of Safeguarding
- Director of Operations of Trust
- Head of IT and Computing
- IT Technical staff
- Teachers
- Support Staff

There is student involvement through the Student Council and Pupil Voice, as well as the SHINE House system.

Educating students in e-safety
A clear objective of the College is to educate students in safe use of IT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

Students will receive specific e-safety lessons aimed at ensuring that:

- Students know the e-safety risks that exist and how to identify when they are at risk.
- Students know how to mitigate against e-safety risks by using e-safe practices whilst online.
- Students know when, how and to whom to report instances when their e-safety may have been compromised.



- Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

The College will follow the ThinkUKnow programme by the government's Child Exploitation and Online Protection (CEOP) centre as one of the primary education tools. In addition to this specific training all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

Photographic, video and audio technologies

- Mobile phones are banned from the College site unless prior permission has been sought by the parent/ carer. In this instance, students will hand the mobile phone in to Student Services for secure storage during the school day. The 6th form students are exempt from this ban and they may bring their phones to College providing that use of the phones is appropriate to their learning environment.
- Staff must check to ensure that the College has permission for the image of any student to be captured on an electronic device.
- Staff may use photographic or video devices in curricular activities and on school trips/ visits. All images captured must be stored and downloaded onto the College network drive and then deleted from these electronic devices.
- Students may not take images of other students whilst on the College site using any electronic device unless given permission by a teacher in a curricular activity (this will be a device provided by the College specifically for this purpose).

Responsibilities for E-safety

Within the College all members of staff and students are responsible for e-safety. Responsibilities for each group include:

Students will:

- Participate in and gain an understanding of e-safety issues through e-safety training sessions in IT classes and in pastoral sessions.
- Comply with a highly visible student's Acceptable Use Policy (AUP) which students must agree to and sign to acknowledge this in their planners.
- Report any e-safety issue to the teacher, form tutor, Head of Year or parent.
- Take responsibility for their own actions, using the internet and communications technologies appropriately and safely.

All Staff will:

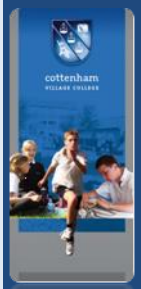
- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.
- Report any e-safety issues to the Safeguarding Lead as soon as the issue is detected.
- Comply with a highly visible staff Acceptable Use Policy (AUP).

Teaching Staff will:

- Educate students on e-safety through specific e-safety messages in lessons which rely on IT and use of the Internet and re-enforcing these messages in the day to day use of IT in the classroom.

The ICT support team will:

- Ensure that the best technological solutions are in place to ensure e-safety as far as possible whilst still enabling students to use the internet effectively in their learning.
- Check that virus protection is installed and updated regularly.



- Manage student access to WIFI with secure passwords and regular security checks on its use. Only students with equipment supplied for specific educational needs have access to the WiFi and any such devices are managed from a central point.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, securing and preserving evidence of any e-safety breach.
- Will use internet filtering to block inappropriate content and block websites which are irrelevant/ inappropriate to the student's programme of study.
- Check and audit all systems to ensure that no inappropriate data is stored or is accessible.
- Work with the Deputy i/c of Safeguarding and the Director of Operations to create, review and advise on e-safety and acceptable use policies.
- The academy will use a system which tracks all student activity on the academy's computers. This system will automatically flag potential e-safety issues which will be monitored and then can be investigated by the support for learning team.
- Monitor the technology systems which track student internet use to detect e-safety breaches.
- Assist in the resolution of e-safety issues with the E-Safety Deputy and the Head of IT and other members of staff as appropriate and required.

IT and Computing Head of Faculty will:

- Lead the development of the e-safety education programme for students and staff.
- Support in reviewing emerging technologies and any potential aspects that will need reviewing in light of the AUP policy.

E-Safety Deputy will:

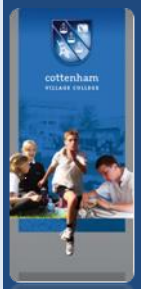
- Deal with e-safety breaches from reporting through to resolution in conjunction with the ICT support team.
- Work with the Director of operations, the IT technical staff and Head of Computing and IT to create, review and advise on e-safety and acceptable use policies
- Work with outside agencies including the police where appropriate.
- Maintain a log of all e-safety issues.

How the College will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher. If the Headteacher is reported for any misuse it will be reported to the Executive Headteacher, and if the Executive Headteacher is reported of misuse it will be reported to the Chair of The Board Trustees.

Where there is an instance of misuse, the following procedures apply:

- Complaints of Internet misuse will be dealt with at a senior level.
- Any staff misuse will be referred to the Headteacher.
- Complaints which relate to any area of Child protection and safeguarding must be referred through the usual channels and involve the Designated Persons at the College
- Illegal misuse of the Internet or electronic devices will be reported to the Police



Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.
- Students will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'.

Working with parents and the community

Many students will also have access to ICT and the internet at home, often without some of the safeguards that are presents within the academy environment. Therefore parents must often be extra vigilant about their child's e-safety at home.

One of the goals of the College is to support parent's role in providing an e-safe environment for their children to work in and outside the College. The College will do this in several ways, such as publishing e-safety information and direct parents to external e-safety advisories via the College website and Parentmail.

The College will seek to provide information and awareness to parents and carers through:

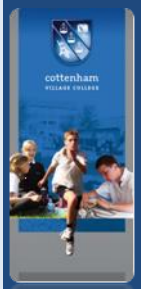
- Letters, newsletters, CVC web site
- Parents / Carers evenings
- Reference to the relevant web sites / publications www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the LGB on :	20/11/15
The implementation of this e-safety policy will be monitored by the:	E-safety Committee Personnel Committee Trustees
Monitoring will take place at regular intervals:	Once a year
The Personnel Committee will receive a report on the implementation of the e-safety policy generated by the E-Safety Committee (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	20/11/16
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LADO, LA Safeguarding Officer, POLICE

Appendices

- Student Acceptable Use Policy Agreement
- Parents / Carers Acceptable Use Agreement
- Staff Acceptable Use Policy



Appendix: Acceptable Use Policy – Students

- **I understand** that Cottenham Village College will monitor my use of the systems, devices and digital communications.
- **I will –** be respectful to everybody online; I will treat everybody the way that I want to be treated.
- **I promise –** to show respect for the digital work that other people have done.
- **I promise -** that the messages I send, or information I upload, will always be polite and sensible.
- **I will not -** use technology to harass, harm, offend or insult others.
- **I will not** – share personal information online with anyone.
- **I will not** - install or attempt to install programmes of any type on a school machine without staff permission.
- **I will not** – damage the IT equipment, if I accidentally damage something I will tell my teacher.
- **I will not -** attempt to access, alter, move or delete another pupil's file or disrupt their learning in any way.
- **I will not -** post pictures or videos of others without their permission.
- **I will -** take care of my online reputation and make sure my photos will not embarrass me in the future. I understand that photos, once posted publically, are impossible to delete.
- **I will not** – use or share other people's usernames or passwords.
- **I will not -** use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are illegal, obscene, harmful, offensive, or abusive.
- **I understand -** that some websites, social networks, video games have age restrictions and I should respect this.
- **I will -** only email staff members using the school email system.
- **I understand -** that I must be careful when copying materials from the web and I am aware of the issues surrounding plagiarism.
- **I understand -** that there are sensible time limits when using technology (computers, games console, media devices).
- **I promise -** I will not allow technology to affect my health / sleeping times.
- **I will** – let my teacher know if anybody online asks me for personal information.
- **I will not -** respond to hurtful or upsetting messages, **I will** – let my teacher know if I receive a message which is hurtful or upsets me.
- **I understand –** that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
- **I understand -** if I need to report any abuse I will report it to a parent or carer, teacher or trusted staff member. If I cannot tell one of these people about online abuse, I will use an organisation such as Childline, or click the CEOP button to report the abuse.

Signed (Student): **Date:**

Appendix: Acceptable Use Policy – Parent / Carer

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That Cottenham Village College and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The College will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children.

Use of Cloud Systems

Cottenham Village College uses Google Apps for Education for students and staff. This permission form describes the tools and student responsibilities for using these services. The following services are available to each student and hosted by Google as part of the school's online presence in Google Apps for Education:

- **Mail** - an individual email account for school use managed by the school

- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments.
- **Docs** - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office.
- **Sites** - an individual and collaborative website creation tool

Using these tools, students collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The College believes that use of these tools significantly adds to your child's educational experience. As part of the Google terms and conditions, we are required to seek your permission for your child to have a Google Apps for Education account.

Use of Biometric Systems
The school uses biometric systems for the recognition of individual children in the following ways.

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints / palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Permission Form

Parent's / Carer's Name:

Student's Name:

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school, including Google Apps for Education.
I acknowledge that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

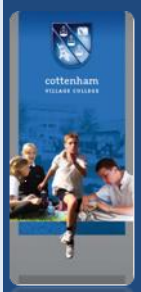
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Yes / No: I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No: I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No: I agree to the school using biometric recognition systems, as described above. I understand that the data cannot be used to create a whole fingerprint / palm print of my child and that these data will not be shared with anyone outside the school.

Signed: Date:



Acceptable Use Policy for Staff

Computers, laptops and other networked resources, including Internet access, are available to staff in the school. **These resources are intended for educational purposes, and may only be used for legal activities consistent with the rules and policies of the school.** It is expected that staff will use computers as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the use of the online curriculum. The computers are provided and maintained for the benefit of all staff, who are encouraged to use the online resources available to them.

Unacceptable Use of ICT Facilities and Monitoring

Inappropriate use is any use prohibited by the terms of this policy or use determined by the College's system administrators to be inappropriate under particular facts and circumstances.

1.1 Posting, creating, accessing, transmitting, downloading, uploading or storing any of the following material (unless it is part of an authorised investigation) will result in disciplinary action being taken (this list is not exhaustive):

a. pornographic or sexually suggestive material or images of children or adults which may be construed as such in the circumstances (that is, writing, texting, pictures, films and video clips of a sexually explicit or arousing nature); or

b. any other type of offensive, obscene or discriminatory material or criminal material or material which is liable to cause distress or embarrassment to the Academy or others.

1.2 The contents of our ICT resources and communications systems are our property

1.3 The College reserves the right to monitor, intercept and review, without further notice, usage of our IT resources and communications systems, including but not limited to telephone, email, messaging, voicemail, CCTV, internet and social media postings and activities, to ensure that our rules are being complied with and for the following purposes:

a. to monitor whether the use of the email system or the internet is legitimate and in accordance with this Code;

b. to assist in the investigation of alleged wrongful acts; or

c. to comply with any legal obligation.

1.4 By using the College's resources and systems, the user is agreeing to the possible monitoring of all forms of communication. We may store copies of data or communications for a period of time after they are created, and may delete such copies from time to time without notice. If necessary, information may be handed to the police in connection with a criminal investigation.

Staff Agreement

I have read and understand the above and agree to use the College computer facilities at Cottenham Village College within these guidelines.

Staff Name:

Staff Signature:

Date

Policy Document

Cottenham Village College

This policy was ratified on .....

and will be reviewed on .....

Signed by the Headteacher / Chair of Governors .....