Authors: BLO, AK
Editors: JAR-C, EL
Created: 6/20
Version: 29/11/25
Review: 31/8/26

Digital Safety Policy
Incorporating Staff and Student Acceptable Use Policies

To be read in conjunction with the *Safeguarding and Child Protection Policy*; *Nudes and Semi-Nude Policy*; *Student Digital Safety Policy*; *Remote Learning Policy*; *Online Activity Policy and Procedures*

Aims

This policy aims to reduce risks to personal safety and well-being from **Content**, **Contact**, **Conduct** and **Commerce** (the 4Cs) as outlined in paragraph 135 of KCSIE 2025 when using fixed and mobile communication devices that allow access to the internet including: personal computers, laptops, tablets, mobile phones and gaming consoles.

We aim to:

- protect your data following the GDPR (2016) and Data Protection Act (2018) and UK Data (Use and Access) Act 2025.
- protect Fundamental British Values;
- eliminate radicalization as required by the Prevent Duty;
- meet our Safeguarding duties as outlined in KCSIE 2025 and the Online Safety Act (OSA) 2024 such as preventing Cyberbullying and Online Sexual Abuse which includes:
    - Sexting/Youth produced sexual images;
    - Upskirting;
    - Cyberflashing;
    - Intimate Image Abuse (Revenge Porn);
    - Deepfakes;
    - Flashing Images (strobe effects);
    - Online Threats;
    - Encouraging Self-Harm;

This policy is directed to all Staff, Students, and Parents who use digital media in the School context.

Emboldened references to **Staff**, **Students** and **Parents** are for that group’s special attention.

Personnel

The School’s Digital Safety Coordinator is the Safeguarding Lead (DSL). The Information Manager and Network Manager assist with Digital Safety programs such as filters and firewalls and monitor access levels using audit tools from the Southwest Grid for

Learning (SWGfL). The Digital Safety Committee meets termly to discuss all aspects of digital safeguarding.

Digital Safety Committee

The Digital Safety Committee consists of:

- DSL
- Data Protection Officer
- Information Manager
- Heads of Houses
- Head of PSHE
- Head of Juniors
- Head of IT
- Music Dept rep
- Heads of School
- Facilities and Site Manager

This committee meets termly to discuss and review policies and consider current social media trends. From these discussions a series of assembly/tutor group materials are produced to educate students about Digital Safety concerns.

The minutes from Digital Safety meetings are shared with the Joint Principal (NS) and the Safeguarding Governor immediately following the meeting. The Digital Safety meeting minutes form part of the DSL's Report to Governing Body meetings. The Committee has the support of, and has received INSET from, the Digital Safety lead from the Manchester Safeguarding Partnership Digital Safety also forms part of the whole staff Safeguarding training.

The Committee produces information for students, staff and parents in separate sections on the school intranet and in the **Parent Gateway**. Posters are placed strategically around School to remind students to behave appropriately online. **Students** have a reporting 'button' ('Be Safe') on the homepage of the Student Intranet which directs concerns to the DSL. Students are also encouraged to use other reporting routes such as CEOP.

The Digital Safety committee will regularly audit ICT use to establish if the *Digital Safety Policy* is adequate and that the implementation of the *Digital Safety Policy* is appropriate. For example, the SW Learning Grids 360° Digital Safety audit tool; OFSTED Digital Safety leads update.

Parents

The *Digital Safety Policy* will be mentioned in newsletters, new student information and a copy is available on the School website.

Information and guidance for parents on Digital Safety, such as online challenges and hoaxes, will be made available through the **Parents'** Gateway and to **students** via the School's intranet and **Student** Gateway.

Images that are published in promotional literature and on the School's website that include students will be carefully selected. **Parents** are asked to opt out if they do not wish their child's image to be used.

Parents are expected to monitor their child's online use and to offer guidance in keeping with this policy so that students are safeguarded from digital harm at home and at school.

Network Services

Chetham's provides access to workstations (desk & lap-top) and respects the law as it applies to computer services on or off the School's site, but makes no warranties of any kind, whether expressed or implied, for the service it provides and cannot be held responsible for:

- any loss or disruption to network/internet services;
- any damage or loss suffered through such usage including but not limited to:

  a. personal devices
  b. hardware or software problems
  c. user errors or omissions
  d. financial obligations arising through unauthorised use of its network services.

Hardware

- Please report any problems to ITSupport@chethams.com
- Damage caused to hardware on or off site, deliberately or accidently, may be chargeable
- School equipment may only be taken off site for **staff** work-related purposes and if covered by their personal insurance. **Staff** are responsible for the equipment while it is off site
- If **staff** wish to purchase IT hardware for their professional/departmental use, please see the Information Manager
- School laptops should have up-to-date Windows Firewall and Defender enabled
- Use of your own devices at School and/or connecting to the School network is at your own risk.

Internet Services

- Use of the internet is at your own risk. Chetham's accepts no responsibility for the accuracy or quality of the information obtained using its internet services
- All network activity and online communications are filtered and monitored, including personal and private communications made via the School Network.

Filtering and Monitoring

Network and Internet use, including emails, is monitored digitally and can be traced using the School's internet filter Opendium, audit tools and AB Tutor. Kaspersky protects the School Network from malicious software. All data traffic on the Network is encrypted to guard against cyber-attack. The internet filter is checked weekly for breaches and efficacy, and data is shared with, and reviewed by, the Pastoral Management Team. A report is prepared for the Digital Safety committee, and Safeguarding committee which is then overseen by the governor for safeguarding and child protection and reported to the Governing Body.

Type of monitoring	Frequency	Completed by	Actions
Microsoft 365 compliance filter	Daily	ICT	Report sent to all HoS
Opendium	Daily. Additional monitoring prompted by specific concerns	**HoS/HoH rota:** Mon – HoS M Tues – HoS J Weds – HoS J Thurs – HoS M Fri – HoS S Sat/Sun – HoH	Concerns shared with relevant HoS/HoH and DSL. CPOMS entries. Staff concerns to JP (NS).

	using X and Y reports		
Opendium/Kaspersky	Blocked website and malware reports	ICT	Concerns shared with relevant HoS/HoH and DSL. CPOMS entries.
Concern form completed by a staff member	Ad Hoc	DSL asks HoS for a Opendium report	Concerns shared with relevant HoS/HoH and DSL. CPOMS entries.
Direct report (verbal, e-mail, teams)	Ad Hoc	Concern passed to HoS on daily rota to investigate	Concerns shared with relevant HoS/HoH and DSL. CPOMS entries.
Be Safe button on intranet	Ad Hoc	Concern passed to HoS on daily rota to investigate	Concerns shared with relevant HoS/HoH and DSL. CPOMS entries.
Anonymous boxes in XYZ	Ad Hoc	Concern passed to HoS on daily rota to investigate	Concerns shared with relevant HoS/HoH and DSL. CPOMS entries.
Key word review	At half-termly digital safety meeting and/or in response to current events (such as an emerging trend of concern)	Digital safety committee	Key word list updated
Digital safety meetings	Half-termly intervals	Digital safety committee	As required

We are advised by our filtering and monitoring partner Opendium and are also in conversation with the UK Safer Internet Centre. Opendium scrutinises the functional identifiers which lie in the background of applications and websites such as Netflix.

Opendium has a Generative AI filtering category which aims to block stand-alone generative AI websites. This is a work in progress. We are also working with them on filtering AI embedded in other applications. In this scenario the best option is for users to turn off the AI features, if that is possible.

Students will be allowed access to age-appropriate apps. **Parents** are requested to ensure that their child does not have access to sites which are not appropriate for their child's age and stage. For example a site with a 13-year-old restriction such as Microsoft Copilot means that the person accessing the site has to have reached their 13th birthday before gaining access.

Internet Use in the Curriculum

Internet use is not only part of the statutory curriculum and a necessary tool for learning but also a part of everyday life for education, business and social interaction. As such the School has a duty to provide students with Internet access as part of their learning experience.

We also recognise the need to educate students to use the Internet safely, securely and independently outside of the School context. The curricular vehicles for digital literacy are ICT lessons for the Lower and Middle School. **Students** will be educated:

- in the safe use of the Internet for research, including the skills of knowledge location, retrieval and evaluation in Y7-Y8 ICT lessons.
- to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- to acknowledge the source of information used and to respect copyright when using Internet material in their own work. In particular teachers responsible for assessing coursework will explain to students why plagiarism (the use of others' work, including AI generated text and images without acknowledging the source) is not allowed
- to remain safe online, including awareness of the dangers of generative Artificial Intelligence which includes generative tools such as ChatGPT and chatbots.

The School's internet access is designed to enhance and extend education by the promotion of safe and useful content by teachers, for example, links and content placed on our VLE, Moodle, eStream, Teams and Office 365.

The PSHE and ICT programmes, and Tutor groups covering both safe School and personal use. Digital Safety sessions provide a safe environment for debating issues such as radicalisation, sexting and digital Safety, which in turn are reinforced in other areas of the curriculum e.g. Fundamental British Values in PSHE and History.

Digital Safety is a termly topic in Year group assemblies, Tutor periods and House activities and covers the 4 Cs including, but not limited to:

1. **Content** which is illegal, inappropriate or harmful (including extremism, misinformation, disinformation, fake news and conspiracy theories)
2. **Contact**: harmful online interaction with other users
3. **Conduct**: harmful online behaviour such as bullying or sharing inappropriate images
4. **Commerce**: inappropriate advertising, financial scams, gambling.
(see paragraph 135 of KCSIE 2025 for full details)

The annual Digital Safety week is celebrated to help raise the profile of safer internet use.

Chetham's teaching **staff** should contact the DSL in advance of lessons relating to Digital Safety content that may impact our students e.g. mental health issues such as self-harm and eating disorders.

Use of Artificial Intelligence (AI) Programs

Generative AI is ubiquitous. We cannot guarantee that our students will not use AI in some form. Instead we aim to educate our **staff**, **students** and **parents** about the pitfalls of AI, including approaching AI generated content critically, verifying sources, data and logic before using as part of studying or decision-making. The human individual's voice should be evident throughout any AI-assisted content. AI used in school is staff-approved and age appropriate.

Copilot is now integrated with Microsoft 365 which we all use in our School. It has been comprehensively tested by our IT Support Team and DSL. Student accounts are carefully configured by our technicians. We train our students and staff not to share personal data with Copilot. Staff do not use Copilot for making final decisions about cases. Whilst at School students can use Copilot under supervision, for example in year 7 and 8 ICT lessons Copilot is used to help programming in Python. However, students cannot use Copilot without supervision unless they are over 13 and their parents have given them permission to use it. Copilot is designed to put student safety and privacy first with 'Enterprise-grade data protection' such as encryption at rest and in transit. Student data is not used for AI model training and there are no personalised ads or experiences for users aged 13-18. Our IT administrators are able to enable/disable Copilot Chat for students.

Whilst we do not currently use any other Artificial Intelligence products with students we are aware of our responsibilities should we use them in the future.

Any such AI products will be vetted and will need to meet the Age Appropriate Design Code; the DfE's Product Safety expectations; and the following minimum criteria, before we use them:

- Prevent access to harmful and inappropriate content
- Robust activity logging procedures
- Secure against malicious use or exposure to harm
- Robust data handling and transparency around processing of personal data
- Does not collect or store intellectual property created by students or copyright owner for commercial purposes
- Transparent systems which safeguard children by design
- Accountability and human oversight
- Ongoing Risk Monitoring
- Meet our Safeguarding and legal duties

We will not use AI to make decisions without human oversight. AI may be iused to assist staff in their roles, but all such outputs will be reviewed for accuracy and appropriateness by staff.

Security

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. The School Network Manager will maintain a current record of all staff and students who are granted access to the School's electronic communications.

Staff must read, sign and agree to the Staff AUP before using any school ICT resource.

Students must read, sign and agree to the Student AUP before using any school ICT resource.

Parents will be asked to sign and return a consent form for student access.

Software installation on School PCs is controlled by the Network Manager.

Tips for improving the security of your account and data include:

- Keep your login details secret. If you use someone else's ID and password you will have your services suspended and the matter will be referred to the Leadership Group. If yours is compromised, please inform the IT Department.
- Use strong passwords (8 characters +, with a mix of alpha-numeric and special characters) for access to the network and School programs.

- Lock or log out of your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes places using your credentials.
- Ensure that sensitive data is not visible to others.

Personal data sent over the Internet through the Staff and Student Intranets and the Parent Gateway is encrypted. **Staff** are encouraged to use the Staff Intranet; Sharepoint; Remote Access Desktop and MS OneDrive to access documents rather than taking physical media/hardware out of school.

Staff designated directly by the Joint Principal (NS) may lawfully search, screen or confiscate electronic devices, without consent or parental permission, if there is a suspicion that the student has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Staff will alert the DSL about any suspicious data, files or images that are believed to be illegal. These will be passed to the police as soon as practicable, including nude or semi-nude images of children, without deleting them. Staff should **not** view the images.

Any data, files or images which are a cause for concern but not believed to be unlawful, may be deleted or may be kept as evidence of a breach of the school's behaviour policy. In such cases the device in question will be kept in a safe place preferably visible to the owner, e.g. in an envelope on a desktop of the member of staff who has discovered the concern. Any material that the School believes is illegal will be reported to appropriate agencies such as (but not limited to) SWGfL, CEOP, FACT, ICO and the Police.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR (2018) and Data Protection Act (2018), and only shared with authorised agencies upon request (see *Data Protection Policy* and *Privacy Notices*).

.

- Personal information is anything relating to a person that can be used to identify them. This includes both physical paper and electronic/digital records, including but not limited to:

  a. Names of staff and students;
  b. Dates of birth;
  c. Addresses;
  d. National insurance numbers;
  e. grades and marks for schoolwork;
  f. Medical information;
  g. Exam results;
  h. SEN assessments and data;
  i. Staff performance management reviews.

- Data containing the personal information of staff or students must not be stored on any electronic device outside of school without being encrypted and must comply with the GDPR. Secure access to documents and systems is available through the Staff Gateway and One Drive.

- Any data stored or transferred on a removeable device must be encrypted and may only be transferred to School equipment. Encrypted drives are available from the IT dept.. For data protection purposes you must not take the USB drive out of the EU. If you lose the USB drive please inform the Data Protection Officer.

Photos and videos of students must only be taken using School owned devices. Any exception to this can only be authorised by the Joint Principal (NS). As part of our school activities, we may take photographs and record images of individuals within our school. As per the *Data Protection Policy*, 'we will obtain written consent from parents/carers/guardians for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer/guardian and student.' **Staff** should

- Delete unwanted files in line with the school's Data Retention policy.
- If **Staff** mobile device(s) to access school email you must make sure that they are protected with a password or pass-code logon. If your device is lost or stolen you must inform the Data Protection Officer as soon as possible.
- When **Staff** contracts end or **Students** leave their network, email and other systems will be disabled.
- **Staff** should immediately report any **breach** of information to the Data Protection Officer. (See *Data Protection Policy* and *Privacy Notices*).

Email

Staff and students should only use official school email accounts (@chethams.com); School-based MS Teams communications; or communicate via the Music Office/General Office or Houses. If a student receives communication from any member of staff other than through these channels they should tell their Head of House or Head of School immediately.

Students must immediately tell a teacher if they receive offensive email. Students should not reveal personal details of themselves or others in email communication or arrange to meet anyone outside of school without specific permission from staff or parents.

Students and most **staff** are not permitted to use school-wide distribution groups on the school email system.

Students must always use email in line with the behaviour principles outlined in the *Good Behaviour Manual*.

- Office 365 filters School e-Mails; however, think carefully before opening unsolicited, unrecognised emails with attachments.
- Your emails and online activity are monitored.
- Please do not distribute "junk mail"/promotional materials unrelated to School, via School email.
- Please inform the Network Manager (as well as your Head of House/School or Line Manager) if you receive unsolicited emails. Do not send unsolicited emails yourself.
- Please be aware that from time-to-time the IT and Data Protection departments may have to view your School email account for safeguarding and data protection purposes.
- Avoid using personal email addresses to/from School email accounts.

Social Media

The School will control access to social media and social networking sites on classroom and library computers through the Opendium internet filter.

Through assemblies, ICT/PRS lessons and Tutor groups **students** are advised:

- never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, and email addresses, full names of friends/family, specific interests and clubs.
- to consider with great care before placing any images/photos on any social network space. Photos can be copied and changed using AI without the individual's permission. Such deepfakes may be used to embarrass, upset, or blackmail the individual. They should consider how public the information they share is and consider using private areas. They should also consider how background detail and metadata in a photograph or online platform such as Teams might identify the student or their location. Students can disable image features before posting, but this does not guarantee that the image won't be manipulated.
- on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- that comments posted online are often, in effect, permanent and may no longer be owned by them
- to respect others' privacy: personal information, images or videos relating to other people should not be transmitted or posted without the express permission of the person(s) concerned
- that social media can often be used to misrepresent issues and/or as a tool for propaganda e.g. terrorist or extremist groups.

Incidents where social media is used inappropriately by students are recorded by the DSL. Decisions about responses to inappropriate use of social media are taken after discussion with the relevant members of staff and, if necessary, with parents. In serious situations, the School would contact the police directly.

Staff must not accept/request students or former students as friends on Facebook or other social media platforms; and must not actively follow current or former students on any social media platform. Staff use of social media should never compromise their capacity to do their job and they should maintain a professional distance from students just as they would in the physical workplace.

Students must not accept/request staff as friends on Facebook or other social media platforms.

If **staff** social networking posts mention the School in some capacity, then the information posted needs to comply with the following conditions of employment:-

a. Social Networking sites: please use a disclaimer that protects the School e.g. '<u>These are my personal views and not those of Chetham's School of Music.</u>
b. Do not disclose confidential or proprietary information relating to your employment at the School.
c. Respect the privacy and feelings of others. Do not use websites or their equivalent to abuse staff or students. You must obtain the express permission of individuals, who may be connected to the School, in any manner, before posting any written or pictorial details, which reference them. Choose language carefully. (see the *anti Bullying* and *Harassment* policies).

d. If staff suspect any potential conflict of interest, or media contact about site content relating to the School, they should report it to their line manager.
e. Please be aware that the School will take seriously any occasions where internet services are used inappropriately. We expect staff and students to abide by the principles and precepts of the *Code of Conduct* at all times whether in the physical, virtual or electronic worlds.

Cyberbullying

Cyberbullying is the use of information and communication technologies, particularly mobile phones and the internet, to support deliberate, inappropriate behaviour by an individual or group, that is intended to harm another individual or group, either on a single occasion or repeated over a period of time".

Cyberbullying (along with all forms of bullying) will not be tolerated in School. Full details are set out in the School's policy on anti-bullying (see the *Good Behaviour Manual*).

Cyberbullying is covered by the Online Safety Act 2024 and includes, but is not limited to:

- **Cyberflashing:** Sending someone nude pictures online without consent is sexual harassment. It is illegal to send naked images of or to people under 18. If over 18, consent is required

- **Intimate Image Abuse (Revenge Porn):** Sharing or threatening to share intimate images on or offline without consent is illegal.

- **Deepfakes:** where an image or video of someone is digitally altered for malicious purposes including exploitation and possible blackmail of the subject

- **Flashing Images (strobe effects):** Intentionally sending images which flash or contain flashing lights to a person with epilepsy is an offence.

- **Online Threats:** Threats of serious harm online or offline are illegal.

- **Encouraging Self -harm:** Sending content that encourages self-harm or which promotes suicide is illegal.

Taking, using or distributing images of people, their likeness or a suggestion of their likeness, requires their consent. Images, created, curated, used, distributed, edited or adapted without consent, and/or which are against the law, or against the principles of the School's behaviour code will not be tolerated. This includes, but is not limited to, images which are inappropriate, malicious, designed to cause alarm, distress, humiliation or intended for the amusement of others at the expense of one or more other people.

Students can report Digital Safety concerns and cyberbullying issues to the Digital Safety Co-ordinator (Mrs B L Owen) through the School's 'Be Safe' portal on the Student Intranet or by talking directly with her or with any member of staff. A serious Digital Safety concern could be escalated to CEOP.

All incidents of cyberbullying reported to the School will be recorded by the DSL.

Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The School will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Consequences for those involved in cyberbullying may include:

- The bully being asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at School for the user for a period of time.
- Parents/carers may be informed.
- Other appropriate consequences as per the *Good Behaviour Manual*.
- The Police will be contacted if a criminal offence is suspected.

Complaints

Complaints about the School's response to internet misuse will be dealt with under the School's Complaints Procedure.

Any complaint about staff misuse must be referred to the Joint Principal (NS).

All Digital Safety incidents will be recorded by the Digital Safety co-ordinator, the DSL—including any actions taken.

Any issues (including consequences) will be dealt with according to the School's *Good Behaviour Manual* and *Safeguarding and Child Protection Policy*.

Issues concerning data protection should be raised with the Data Protection Officer, Mr Runswick-Cole, via dpo@chethams.com.

Appendix 1

Staff AUP (Acceptable Use Policy) Summary

Anyone who uses the School's ICT facilities or accesses the School wifi through their personal wifi and network enabled devices, are bound by this Policy. Breaches of this policy will be considered by the Leadership Group and may lead to the suspension of services for the user.

Users agree to:

1. take responsibility for their own use of technologies making sure that they use technology safely, responsibly and legally and in line with the AUP.
2. report any known misuses of technology, including the unacceptable behaviour of others.
3. respect the technical safeguards which are in place, keeping network identities open, and only gaining authorised access to systems and services.
4. report failings in technical safeguards or technology.
5. use the School's network resources in a responsible manner that protects the integrity of the School's network and its associated services and does not diminish the service for other network users.
6. the monitoring of network activity and online activity, including personal and private communications made via the School Network.
7. protect their passwords and personal network logins, and to log off the network when leaving work stations unattended and to respect the privacy and integrity of other users' data, reporting any data protection issues to Jon Runswick-Cole, dpo@chethams.com.
8. store or use only software specifically installed on the School Network by a member of the IT Department.
9. Use official School @chethams email accounts for communicating with students on their official School @chethams email accounts.

Users agree **NOT** to:

10. use applications or services which may be used to bring the School, or its members, into disrepute, including but not limited to the posting of information online, the infringement of copyright holders rights and the transmission of unauthorised advertising or promotional materials.
11. upload, download, post, email or otherwise transmit or store any content that is (including but not limited to) unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethnically or otherwise objectionable.
12. collect or store personal information about others without direct reference to GDPR (see School *Data Protection Policy* and *Notices*.)
13. use the School Network to carry out trading, gambling, or other action for personal financial gain, commercial or political purposes.
14. input student, staff or other personal or sensitive data into AI applications such as CoPilot and ChatGPT;
15. use AI alone for decision-making purposes without human oversight

Staff Name:…....................................... Signature..................................

Date: …………………….

For further details see: Digital Safety and Acceptable Use policy; Good Behaviour policy; Safeguarding and Child Protection policy; Counter-bullying policy; Data Protection Policy and Notices.

Appendix 2

Student Acceptable Use of Computers & Mobile Devices

Our aim is to help you become a resilient, skilled, safe and responsible digital citizen when accessing the internet from any communication device, network hardware, software, services and applications. We want you and all members of our community to have a positive online experience.

This code applies to the use of communication devices on or off School premises which affects the welfare of any member of the School community, or where the culture and/or reputation of the School, might be put at risk.

Code of Conduct:

1. We make good use of educational opportunities by accessing the internet. We access the internet for educational purposes only during working hours.
2. We stay safe online by keeping personal data, including passwords, and images, private. We respect others' right to privacy and ask for their consent before using, processing, transmitting and/or uploading their data. We do not allow AI to see/use our or others' personal data and images.
3. Our internet activity and emails are recorded and monitored to safeguard us all.
4. We only access material (emails/internet) to which we are legally entitled. We respect copyright laws and age restrictions on websites and apps.
5. We think carefully about what we write/post online or in emails. How would you say it to the person you're writing to / about? Would you be ashamed to show your parents or the Joint Principals? **If in doubt, don't press send**. If you can't say/write/display anything nice, don't say/write/display anything at all.
6. We keep away from abusive, racist, sexist, homophobic, bullying, pornographic, defamatory, criminal or extreme terrorist material. We recognise that any Content, Contact, Conduct and Commerce on line may be risky.
7. We talk to staff if we are concerned about images and other material we receive, send or forward. We report misuse of images; Sexting/Youth-produced sexual imagery; Upskirting; Cyberflashing; Intimate Image Abuse (Revenge Porn); Deepfakes; Flashing Images (strobe effects); Online Threats; and Encouraging Self-Harm because they are criminal offences and Safeguarding issues.
8. If we suspect that we are, or someone else is, being bullied/harassed/intimidated/exploited/blackmailed or radicalised; online or offline, we talk to staff.
9. We use School, not personal email accounts for contacting staff on their School email accounts. Staff use School, not personal email accounts for contacting students on their School email accounts.
10. We use School apps such as MS Teams for teaching and learning purposes only, and not for social messaging, for example in the chat function of a Teams call.
11. We communicate with official school phones; never staff personal phones. School mobile phones or office phones are used by pastoral staff; medical staff; the music timetabler; and staff on School trips to contact you on your mobile phone.
12. We report to staff any deliberately or accidentally inappropriate messages, images or text.
13. We let staff know of any IT problem.
14. We report data protection issues to Mr Runswick-Cole, dpo@chethams.com.

Student Name:………………………………………..
Signature.......................................Date: ………………
For further details see: *Digital Safety and Acceptable Use policy; Good Behaviour policy; Safeguarding and Child Protection policy; Counter-bullying policy, Data Protection Policy and Notices*.

References

https://www.childnet.com

https://www.ceop.police.uk/Safety-Centre/

https://swgfl.org.uk

Data Protection Officer contact: dpo@chethams.com

https://chethamssom.sharepoint.com/sites/StaffIntranet47, also accessed via the Staff Portal: http://www.chethamsschoolofmusic.com/portal.

https://www.getsafeonline.org/protecting-your-computer/passwords/.

CEOP education programme for young people, parents, and schools
https://www.thinkuknow.co.uk

Online Safety Act 2023 (legislation.gov.uk)

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

Is Your Child’s Photo Safe? Understanding Image Consent at Schools and Preventing AI Image Exploitation - Safer Schools NI