Clitheroe Royal Grammar School

Information and Communication Technology and Online Safety Policy

Person(s) responsible: Senior Assistant Headteacher (i/c New Technologies)
ICT Network Manager

Governors' Committee Finance

The primary function of ICT in schools is to facilitate learning. This could be in the classroom, at home, as well as the use of ICT for administration in school to enable procedures to be streamlined. It also encompasses the use of data to inform teaching and learning. This strategy also links closely to the aims of the school including:

- Develop lively, enquiring minds capable of original thought and well-balanced critical argument.
- Become confident, independent learners well-equipped for lifelong learning.
- Derive enjoyment from their learning which should extend their intellectual capacity, develop their interest and stimulate their curiosity.
- Embrace the many opportunities afforded by developments in information and communication technologies, whilst fully accepting the responsibilities that go with using them properly.

This policy reflects the school values and philosophy in relation to the safe teaching and learning of, and with, ICT.

This policy is intended for
- All teaching staff
- All support staff
- School governors
- Parents and carers

Vision

21st century learners live in an ever-changing world where the amount of information and knowledge is growing exponentially. Teachers can no longer be seen as the 'font of all knowledge' as students can access huge amounts of information/knowledge at the click of a button, including artificial intelligence engines (AI). The role of the teacher as facilitator is key; guiding students to explore, think, create and learn for themselves. The experience of the teacher is vital.

Learners need the skills to:

- **SEARCH** for relevant information and knowledge
- **ASSESS** the validity, reliability and bias of that information
- **EVALUATE** material
- **PROBLEM SOLVE** to find solutions logically
- **SYNTHESISE** information
- **CREATE** and **DEVELOP** their own material
- **ENABLE** them to stay safe online
- **ADAPT** to and **EMBRACE** a constantly changing technological world.

Risks
The breadth of online safety issues is continually evolving. To frame our curriculum and training, we follow the DfE's four areas of online risk: **content** (exposure to illegal, inappropriate or harmful content such as pornography, racism, misogyny, self-harm, suicide, antisemitism, extremism or misinformation), **contact** (harmful online interaction with other users or generative AI applications,

including peer pressure and adults posing as children), **conduct** (behaviours that increase the likelihood of harm, such as creating or sharing explicit images and online bullying) and **commerce** (risks such as online gambling, inappropriate advertising, phishing and financial scams).
In line with KCSIE, online safety is treated as a running, interrelated theme in our safeguarding policies; our approach is reviewed at least annually and supported by a strategic plan that reflects the risks our children face.

Our aims for ICT

We aim for all students and staff in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which will enable them to use appropriate ICT resources effectively as powerful tools for teaching & learning. Our learners (students, teachers and support staff) need to be comfortable with and skilful at navigating information and communication technologies.

To fulfil the above aims it is necessary for the school to ensure that:

- there is sufficient access to ICT, especially the internet and Wi-Fi
- ICT experiences are focused on enhancing learning
- skills (stated above) are embedded in the curriculum
- all users understand how to be safe (including personal safety, security of data etc.)
- there is a relevant Computing curriculum including Computing lessons and ICT used throughout the curriculum
- e-safety is embedded in the curriculum and the school works with staff, students and parents such that all parties know how to behave safely online
- students are safe from extremist material (appropriate filters are in place in school) and that the school is vigilant at monitoring students who are vulnerable in this area, providing access to support and information
- students and staff are aware of the opportunities, limitations and dangers of using Artificial Intelligence systems
- support and guidance from ICT specialists/technicians
- resources and equipment are kept up to date as much as possible
- all ICT is secure that is used in an appropriate manner
- cross curricular links are exploited where appropriate
- the guidance for the use of AI is clear and communicated to both staff and students

Curriculum Development & Organisation

All students have Computing lessons in Years 7, 8 and 9, where they learn to use software packages and AI creatively, how to code and also learn about how to be a safe and responsible computer user. As well as the timetabled Computing lessons, a two-weekly online booking form is available for staff of all departments to sign up for additional time where appropriate.

In addition:

- Students learn about online safety in Computing lessons.
- Personal safety, online behaviour and financial security is also covered in the Personal Development curriculum as well as whole school assemblies
- Targeted assemblies are used to address online issues within different year groups
- The pastoral teams (and all staff) are also trained to handle online issues with sensitivity, care and professionalism.

All staff are allocated their own personal laptops/netbooks as well as each teaching room being equipped with a PC and a digital projector. In addition, individual machines in staffrooms and departmental offices also support the development of ICT capability.

ICT Management and Support

The school provides an appropriate level of support staff consisting of a network manager and two network technicians to maintain and support our resources.

It is important that hardware resources are maintained. It is intended, therefore, within budget constraints, to upgrade/replace equipment on a regular basis and annually sign up to Microsoft school agreement to ensure all operating systems and application software is also up to date.

The school is committed to provide staff training on ICT to encourage and build confidence in the use of ICT. Training is provided by the Deputy Headteacher i/c New Technologies, departmental staff with expertise and the ICT technical team. Requests for training on any of the school's ICT resources are welcomed. Third party ICT training is also available for staff development.

Students are encouraged to make responsible use of ICT and the school has acknowledged the need to ensure that all students are responsible and safe users of the Internet and other communication technologies. Student **Computer and Internet Use Statements and the school's Mobile Data device Policy** have been drawn up to protect all parties.

Filtering and Monitoring

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered Fortinet by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. Where generative AI tools are used, the school will ensure that the same safeguarding, filtering and monitoring expectations apply. There is a clear route for reporting and managing changes to the filtering system.

The school operates a variety of monitoring strategies to minimise safeguarding risks on internet connected devices. These include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software
- CCTV to monitor computer rooms

DfE Keeping Children Safe in Education requires schools to have "appropriate monitoring" and the DSL (Main School) and the Network Manager regularly review the DfE published 'Filtering and monitoring standards for schools and colleges' published by the DfE (March 2023), using the filtering and monitoring checklist.

ICT Security

The objective of ICT security is to ensure school's continuity and minimise damage by preventing and minimising the impact of security incidents.

The purpose of the policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.

It is the school policy to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- regulatory and legislative requirements will be met
- senior leaders are informed about attempts to breach the computer filter
- Staff are reminded about ICT security at regular intervals

Technical Security

- Servers, wireless systems, and cabling are securely located and physical access restricted.
- There are rigorous and verified back-up routines (see Appendix 1)
- Appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.
- The school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- All users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves.
- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school's IT Support Team regularly monitors the activity of users on the school technical systems and users are made aware of this in the acceptable use agreements
- Users report incidents to the IT Team or SLT and the IT Team report any activity which contravenes the IT or Behaviour Policies to SLT
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Remote network management tools are used by staff to control workstations and view users' activity.
- By default, users do not have administrator access to any school-owned device.
- The school has an alarm system installed throughout.
- There are also CCTV cameras in all Computer Rooms to enable identification of students if needed.

Monitoring and evaluation

It is the responsibility of each member of staff to adhere to the policy, standards and procedures.

The Deputy Headteacher (Main School), working closely with the Network Manager and Head of Computing, has direct responsibility for maintaining the policy, standards and procedures and providing advice on their implementation.

Procedures for ICT and online safety:

Appendix 1 – ICT Backup Procedures

Appendix 2 – ICT Statements for Staff and Acceptable Computer, Mobile Device and Internet Use Statement For Main School Students and Sixth Form Students

Appendix 3 – Safeguarding Remote Learning Guidance

Appendix 4 – Filtering and Monitoring Procedures

Appendix 5 - Computing / ICT Staffing Structure and Requests Procedure

Date of last review:	October 2026
Date of approval by Governors:	October 2026
Date of next review:	October 2027

ICT Backup

The data on our four main servers are backed up in the following way:

3 Servers Based at the York Street Site Using LTO Tapes: -

- A backup is taken every weekday evening
- Monday to Thursday: an incremental backup
- Friday: A full backup

The Friday rotation consists of 3 tapes:

- Friday 1 to 3

Friday tapes 1 to 3 are used in sequence.

All tapes are stored off-site.

The backups are checked each morning with the restoration of a file.

1 Server Based at the Chatburn Road Site Using Off Site Using NAS: -

- A backup is taken every weekday evening
- Monday to Thursday: an incremental backup
- Friday: A full backup

The Friday rotation consists of 3 backup areas:

- Friday 1 to 3

Friday areas 1 to 3 are used in sequence.

The NAS is stored off-site.

The backups are checked each morning with the restoration of a file.

Information, Communication and Technology Statement (and Guidelines) for Teaching and Support Staff

Meanings

1. **school** means: Clitheroe Royal Grammar School (CRGS) as directed by its Governors, Headteacher and Senior Leadership Team (SLT)
2. **network/systems** means: any computer hardware or software owned, rented or leased by the school and made available to any teacher or support staff employed, whether directly or indirectly, by the school
3. **user** means: any person who uses the school's systems with the permission of the school either expressly or by presumption
4. **internet** means: the world wide web whether accessed online or offline by way of stored files, images or moving pictures howsoever stored and to include portable storage devices
5. 2 and 4 above can collectively be referred to as "**IT resources**"
6. **removable storage device** means: compact discs, DVDs, USB sticks, flash media or any other media that is capable of storing files, data, images, whether moving or still, or any other information that can be viewed or transferred from the device.

The use of the school's systems by the user is a benefit of the user's employment and one which the school actively encourages to enhance their contractual obligations for teaching and learning. Any deliberate breach of this policy will amount to a breach of the user's terms of employment and may result in sanctions being enforced under such contract of employment whether expressly or implicitly incorporated into the same.

The school retains and incorporates its absolute right, and will exercise the same at its absolute discretion, to monitor, by whatever means it deems suitable, all systems and internet access records stored on, or processed through, any school network or system or the CRGS and/or School Broadband servers.

Accordingly the school has determined the following rules and guidelines for the use of its IT resources which may be amended as and when the school deems fit to do so.

Rules

It is forbidden for a member of staff to:

1. deliberately disclose any information to an unauthorised person or organisation which is contained on the school's network. An unauthorised person or organisation is any entity not directly connected to the school's Senior Leadership Team or any entity who the user does not truly believe is entitled to receive such information
2. access any user accounts other than by their own authorised accounts and password or deliberately disclose the same to another person, save, that person having express permission, or implied permission by the nature of their employment description, from the Headteacher / SLT to do so
3. access any files, data or other resources of other users which may be stored on the network unless such files, data or resources are open for common view in public / shared areas
4. deliberately engage in any activity that affects, or threatens to affect, the integrity of the network or any files, programs or systems contained thereon
5. deliberately send an e-mail or post online (e.g. on Facebook, Instagram) any message that contains, or has an attachment which contains, defamatory, insulting, offensive, racist, violent or threats of violence, indecent and/or obscene words or images, chain letters or any other

item that the user should reasonably know is an unacceptable subject, image or content within a school environment or that is likely to bring the name of the school into disrepute

6. view any indecent / obscene, racist or violent material on the school's resources, to include laptop computers whether on school premises or not
7. use the school's IT resources for personal financial gain, gambling, promotion of personal political views or advertising anything that the user has not had prior written permission from the Headteacher or Governors to advertise
8. use the school's IT resources to access any chat room or forum not hosted by an educational site recognised by SLT and / or the Local Authority
9. use the school's IT resources to post anonymous messages on any system or network
10. download any third party unlicensed program or file from the internet or removable storage device without written permission from the Headteacher / Network Manager / Computer Technician
11. copy programs or data which the user does not have authority to do so. The copyright of all materials used should be respected.
12. publish, or cause to be published, whether directly or indirectly, on the internet or via e-mail any material or data which identifies, whether directly or by implication, Clitheroe Royal Grammar School, its staff, governors or pupils, whether past or present, without the full written permission of those persons identified and the Headteacher.

Members of staff should:

1. aim to set up personal social networking sites as private and students are never listed as approved contacts
2. not give their personal contact details to students, including their personal mobile telephone number
3. only contact with students for professional reasons
4. recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible
5. only use school authorised web-based communication (eg Office 365) channels to send messages to a child/young person

General Guidelines

The school offers the following guidance as to the user's use of the school's IT resources to protect both the user and the school:

1. Always keep account names and passwords confidential and change passwords regularly
2. Please use different passwords for each system e.g. SIMS, Office 365 etc
3. Passwords should be a strong password; combination of letters, numbers and special characters and should use both lowercase and capital letters.
4. Always store your files and data in your own secure area on the network or on an encrypted removable storage device (available from the Network Manager).
5. Users should not log on to or use any account other than their own and should log off or lock workstations when leaving them, even for just a short period of time. This includes computers at home if sensitive/confidential school data is being accessed.
6. Ensure your laptop is password protected
7. Back up your files and data regularly, including whilst in use
8. Never access any file, e-mail attachment or program if you are not absolutely sure of its nature or origin or which you do not have the authority to access. If in doubt, do not open it and report the file or program to the Headteacher / Network Manager / Computer Technician.
9. Do not store sensitive/confidential data about students on portable devices such as USB drives, unless the data is encrypted or password protected.

10. Staff should only use password protected/encrypted USB devices in school. These are provided in school on request.

11. Members of staff should also be circumspect in their communications with students so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. This would include using formal language and layout in emails.

Social networking sites guidelines

Employees who choose to make use of social networking site/media are advised as follows:

- Familiarise yourself with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;
- Do not conduct or portray yourself in a manner which may: -
    - bring the school into disrepute;
    - lead to valid parental complaints;
    - be deemed as derogatory towards the school and/or its employees;
    - be deemed as derogatory towards pupils and/or parents and carers;
    - bring into question their appropriateness to work with children and young people.
- Do not form on-line 'friendships' or enter into communication with *parents/carers and students as this could lead to professional relationships being compromised.
- On-line friendships and communication with former students is strongly discouraged particularly if the students are under the age of 18 years.

(*In some cases, employees in schools are related to parents/carers and/or students or may have formed on-line friendships with them prior to them becoming parents/carers and/or students of the school. In these cases, you are advised that the nature of such relationships has changed and that you need to be aware of the risks of continuing with this method of contact. You are advised that such contact is contradictory to the guidelines above).

E-mails

The school recognises that the use of e-mail is a valuable, widely used, quick and cost effective method of communication. It can also be a prolific host for computer viruses, chain letters, pornography and many other items that are unacceptable in the school environment. Users are strongly advised to be extremely careful when utilizing this form of communication.
As such the user is forbidden to:

1. use their official e-mail address other than for purposes of representing the school in an official capacity
2. open or view any e-mail not personally addressed to them using their own authorised e-mail address.

It is highly recommended that the user only uses his/her official e-mail address at all times when communicating with other members of staff, school governors, school trustees, other schools or their staff members and governing bodies, businesses and organisations providing goods or services to the school, internet sites as a direct consequence of the user's research for authorised school activities or other sites whilst representing the school in an official capacity. Use of a personal e-mail address in the preceding circumstances should only be done if absolutely necessary and in circumstances where the user considers it absolutely necessary to perform their duty as an employee.

The school does not encourage, but will allow, the user to send and receive personal e-mails, sent to their non-official e-mail address(es), via the school's IT resources. However, it is the user's full responsibility to ensure that, when sending or receiving personal e-mails via the school's IT resources,

no breach of the rules defined herein is committed. It is highly recommended that the user adheres to the same rules for e-mails sent on their personal accounts as on their school accounts.

It is strongly advised that formal language and layout is adhered to whilst using school email accounts, as members of staff are representing the school in their professional capacity.

Use of YouTube

YouTube can be accessed by members of staff in school. This should only be accessed for educational purposes within school. Staff should ensure that the content is appropriate for use in school before it is shown to students. Members of staff who create videos for YouTube and share with students should be careful to check the appropriateness and publishing settings of all videos on their YouTube channel.

Procedure for photographs of students / staff

If you take photographs of students and / or staff for school events or trips etc, please follow the following procedure:

- after editing photos on your school laptop or home computer, transfer them onto a USB stick
- bring the USB stick into school and have them transferred onto the CRGS media drive located in the Chatburn Road IT office
- please then delete the photographs from your school laptop / home computer and the USB stick
- If photos have been taken using a mobile phone, they should be copied onto the CRGS media drive and deleted from the phone at the earliest opportunity
- for any photos that are used for publications such as the Yearbook, the school website etc, students featured should be checked to see if permission has been given for use of their image. Amanda Moore has the appropriate list.

Use of personal Mobile Phones

See separate policy: Personal mobile device policy

Staff should not communicate with parents or students outside school channels. School channels include Office 365 and EduLink.

Responsibilities

- It is a user's responsibility to look after the equipment that they are using.
- Users should report any broken or malfunctioning equipment to an ICT technician as soon as possible.
- Users are required to respect the privacy of others and the reputation of the school.
- Users should remain vigilant for any breaches of school ICT security and contact the appropriate staff if issues are uncovered.
- It is the user's responsibility to ensure that it does not cause offence or anxiety to others or infringe copyright.
- ICT systems are there for the benefit of the entire institution; activities that waste technical support time and resources are prohibited.
- **All users must sign and return this "Information, Communication and Technology Statement" before using any school's ICT equipment.**

Protocol for investigating matters relating to inappropriate computer use

Students and staff are aware that all computer network use is monitored within school. If there is suspicion of inappropriate use or if it becomes apparent that misuse of the school network has

occurred then this will be investigated by the ICT Network Manager and his staff. Any suspected misuse by staff must be referred to the Headteacher before an investigation takes place. The Headteacher (or, in his absence, a Deputy Headteacher) will always be notified if inappropriate activity and/or material is suspected or discovered.

Protocol for investigating matters relating to students, staff or the school community which may necessitate accessing the internet

On occasion, it may be necessary to conduct an investigation into internet activity which has been brought to our attention.

Most of these investigations will be dealt with by the Senior Leadership Team and the Network Manager, although other staff may be involved with their consent. Any investigation that may require use of the internet must be discussed with the Headteacher (or, in his absence, a Deputy Headteacher) before the investigation occurs.

The Senior Leadership Team and ICT Network Manager would not be required to investigate a matter relating to anything of a sexual nature / inappropriate image as this would need to be discussed with the Lancashire County Council Safeguarding Team and passed on to the appropriate body.

Some social networking sites cannot be accessed via the school network. Therefore, on occasion, the Headteacher (or, in his absence, a Deputy Headteacher) may request that a website is unblocked for a member of the Senior Leadership Team or Network Manager so that matters can be investigated. The Senior Leadership Team and the Network Manager must not investigate any matter without the full knowledge of the Headteacher and / or another senior colleague and the fact finding should be conducted in school.

Following an investigation, printouts may be kept on file if the Headteacher felt it appropriate.

All investigations into inappropriate activity should be logged in a central location.

Student Acceptable Use Agreement

Introduction

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

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect students to agree to be responsible users.
-

Mobile phones and personal smart devices: Students must follow the school's separate Mobile Data Devices Policy.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices and digital communications.

- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will not do anything online that brings the school into disrepute
- Any action that the Headteacher deems damaging to others in the school or out of the school is prohibited.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will follow the rules set out in the Personal Mobile Device Policy.
- I understand that the use of USB mobile devices or any other storage devices that have the possibility of being connected to the school network is prohibited
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- When using the internet for research or recreation, I recognise that:
  - I should ensure that I have permission to use the original work of others in my own work
  - Where work is protected by copyright, I will not try to download copies (including music and videos)
  - When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be

truthful and may be a deliberate attempt to mislead me. Where relevant, e.g. school work, I should reference the website used, time and date accessed and author of the information. This includes the use of Artificial Intelligence tools – effort must be finding the original source of the information used by the AI tool.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school will use the School Behaviour Policy if I am involved in incidents of inappropriate behaviour. This includes when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action, as outlined in the School Behaviour Policy. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- (Sixth Form only) I follow the mobile device policy when I use my own devices in the school e.g. mobile phones, tablets, laptops etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Office 365 applications e.g. Teams etc.

Name of Student: .....
Form: .....
Signed: .....
Date: .....

Parent/Carer Countersignature

Name of Parent: .....
Signed: .....
Date: .....

Agreement of compliance via an online form will be acceptable.

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2023. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.© SWGfL 2023

Safeguarding Remote Learning Guidance

Rationale

Keeping both students and teachers safe when providing remote education is essential. Remote education is a new experience for both staff and students, so it's important that everyone understand how to approach safeguarding procedures online.

Objectives and Suitability

Objectives should be carefully considered and the most appropriate technology selected for the task. This should include a consideration of the age and ability of the students and the number of students. Many students feel they benefit from regular real-time interaction to supplement other learning activities.

Timing of Communication

As always, staff shouldn't communicate with parents or students outside school channels (e.g. they shouldn't talk to parents using their personal Facebook accounts or contact students using their personal email addresses or phone numbers). There is an expectation that the majority of communication with students will be during normal working hours.

Personal Data

It is important to take care not to share personal data (e.g. email addresses). Make use of the BCC function wherever possible, including for groups of students. It is good practice when emailing a group to email yourself and put all recipients as BCC. Staff should take care to handle the information and data relating specifically to students, for example, they should not circulate lists of students yet to complete work.

Communication with Parents / Carers re safeguarding remote learning

Parents / carers will receive regular reminders about online safety. This advice will include setting appropriate security settings, reporting online bullying or abuse and ensuring that any online tuition organised is appropriate and supervised carefully.

Safeguarding

Any safeguarding incidents or potential concerns should be passed to a DSL in the usual way. Any cause for concern regarding the child's safety or wellbeing should be reported to the DSL. This would include possibly abusive behaviour by the parents or other family members, indications of self-harm or bruising, or change in mood or behaviour of the child in question. CRGS's safeguarding policies remain the same regardless of the location of potential danger or abuse. All concerns regarding a student's wellbeing should always be reported to the DSL immediately. The DSL will explore the issue and follow the school safeguarding procedures. If necessary, the DSL can access the Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk.

Choosing an appropriate platform, service or app

There are many useful online platforms that could aid your online teaching. However, before you start, you need to make sure what you're doing is approved and regulated by the school, otherwise, you could be putting yourself or students at risk. Teams is the easiest and safest platform as it sits within the school Microsoft package and students can be invited using their school email addresses. If you

are in any doubt about the suitability of a platform, please check with the Director of Studies (JRE) before use.

Appropriate Access to Online Learning

Always schedule a meeting in advance and end the meeting prior to leaving, ensuring that students cannot be left in a meeting. Never publicise a meeting on social media. By using “meeting options” when setting up your meeting, you can set who can bypass the lobby, to “only me” – this will allow you to control who has access and when to the meeting.

Behaviour and appropriateness of interaction

Teachers should make clear their expectations at the start of any interactive sessions. These should be as close to a ‘classroom standard’ as possible. One particular issue is the protocol for who may speak and when. If this is the first time that classes are delivered online, it may take some time in becoming familiar with the new environment. Make sure that all conversations are: (a) Necessary for the student’s academic development (b) Not involving too personal information (c) Not taking up much more time than you would if you were physically at school (d) Not outside of school hours. All students and parents / carers have a copy of the updated Acceptable Network and Internet Use Statement which has a section added regarding interactive technology. Whilst there should be no one-to-one tuition, it sometimes necessary to speak to a student individually. If this is planned to take place outside of a scheduled lesson, staff should ensure that a member of SLT is aware so that appropriate safeguards can be discussed.

Location/Environment when making recordings or undertaking interactive sessions

There should be careful consideration of the location that everyone uses. Staff should be mindful of their setting when recording broadcasts or taking part in interactive sessions. Pick a neutral area of your home when on video. Make sure to always be wearing appropriate clothing when on camera. Once you’ve chosen the appropriate spot to be on camera, think about what’s in the background. You can change the background to remove any views of your home and replace it with a scenic picture or neutral colour. Young people should also be in an appropriate location within their home – consider what can be seen and heard and whether this is appropriate. It is important to choose a conferencing service that allows the teacher to disable users’ microphone and video cameras; Teams allows you do to this. You should ensure that you are familiar with how to operate these functions before you start any interactive sessions.

Recording and sharing when undertaking interactive sessions

Teachers should make a note of the conference timing and who participated. They should consider if the system includes online chat feature, and if this can be moderated. Consider Privacy settings before posting, e.g. YouTube has a variety of settings (Public, Unlisted, Private, Comments Allowed/Not Allowed) that will determine who can see and comment on any video. It is not acceptable for students to record events. If the service records the conference, make sure that everyone is aware of this. It’s important to know how long any recordings are kept for and how to access them.

Personal Data

If you are using a conference service they may require the sharing of personal data, e.g. usernames to invite in. Students should use school-provided email addresses and create appropriate usernames (if necessary).

Livestreaming Lessons

Livestreaming is transmitting or receiving live video and audio coverage of an event or person over the Internet. When livestreaming face to face lessons to students who are self-isolating at home, teachers must take care to ensure that the camera is focused on the teacher or the board, not the

students in class. Ensure that students are aware that the lesson is being live-streamed to other students outside the classroom.

Recording Segments of Lessons

If you decide to record a segment of a lesson to be shared later with students, for example, an experiment or an explanation, it is vital that students are not captured on this.

Use of personal mobile devices

Personal mobile phones may be used in lessons for school work purposes e.g. photos of classwork, video of practical work, live streaming lessons
They may not be used to photograph students or video students without permission from the Headteacher.
Staff should not communicate with parents or students outside school channels. School channels include Office 365.

Further Guidance:

Getting Started on Remote Learning with Microsoft Teams
https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely
Remote Working: A Guide for Professionals

Further advice and guidance can be found in the "Guidance for Safer Working Practice for those working with Children and Young People in Education Settings"
May 2019 and April 2020 Addendum

Filtering and Monitoring Procedures

Filtering and Monitoring

The school's filtering and monitoring system is delivered by Network Connect and managed by the IT Support Team. Internet access is filtered for all users, and the system is designed to safeguard staff and students by blocking harmful, illegal and inappropriate content. Filtering rules are regularly updated, including the use of the Internet Watch Foundation URL list and other relevant illegal-content lists. The school uses enhanced and differentiated user-level filtering, meaning that different filtering levels can be applied to different groups of users, for example staff and students.

Internet use is logged and monitored to help identify breaches of policy, safeguarding concerns or attempted access to inappropriate material. The school has monitoring systems in place which enable the prompt investigation of potential safeguarding incidents, and outcomes are logged appropriately.

Mobile devices that access the school's internet connection, whether school-owned or personal devices, are subject to the same filtering standards as other devices connected to the school network.

The school operates a range of monitoring strategies to minimise safeguarding risks on internet-connected devices. These include:

- physical monitoring by staff watching users' screens
- live supervision through device-management software
- network monitoring using logs of internet traffic and web access
- individual device monitoring through software
- CCTV in computer rooms

Roles and responsibilities for the management of filtering and monitoring systems are clearly defined and allocated. There is also a defined and agreed process for making changes to the filtering or monitoring system, and this includes the involvement and agreement of a senior leader.

In line with the Department for Education's Filtering and Monitoring Standards and Keeping Children Safe in Education, the school reviews its filtering and monitoring provision at least annually, and checks it regularly to ensure it remains effective, proportionate and appropriate to the safeguarding needs of the school. The DSL and Network Manager regularly review this provision and work with IT staff and service providers to ensure the school continues to meet national expectations.

Where generative AI tools are used, the school will ensure that the same safeguarding, filtering and monitoring expectations apply, and that use of such tools is managed in line with Department for Education product safety expectations.

Appendix 5

Computing / ICT Staffing structure and requests procedure

SLT
James Hoyle – Senior Assistant Headteacher

Teaching and Learning
Matthew Latty – Head of Computing (Teaching)

Network and Support
Darren Vernon – Network Manager
Jon Hill – Deputy Network Manager
Jam Talbot – Computer Technician

ICT Requests
To Darren Vernon, Network Manager and his team
Equipment needs fixing or appears not to be working.
Office 365
Usernames and Passwords (Moodle, email, network)
Acquired software demos to see if it works on the network. Also, Darren will check the licensing.

Telephone
Ext 221(Chatburn Road)
Ext 303 (York Street)
Email
itsupport@crgs.org.uk

To James Hoyle, Senior Assistant Headteacher (j.hoyle@crgs.org.uk)
New hardware
New software (to see if it fits into the bigger picture). If you would like to purchase software for your department, it may be relevant for other departments. Where new software or EdTech processes personal data or incorporates AI, appropriate safeguarding and data-protection checks will be undertaken before approval, involving the DSL and DPO where appropriate.
Proposals for SLT
Requests for IT Training

To Amanda Moore, Data Manager (a.moore@crgs.org.uk)
Requests for class and set lists in Excel
Students having moved sets
Assessment grades and reports systems (SIMS)
SIMS passwords

To Lynne Higginbottom, Bursar (bursar@crgs.org.uk)
Requests for benching and furniture