ICT & Online Safety Policy

Policy Title:	**ICT** (Information & Communication Technologies) **& Online Safety Policy**
Academic Year:	**2020/2022**
Policy Reference:	**G16**
Description:	Framework to ensure the effective and appropriate use of information and communications technology (ICT) & safe online use by all involved with the icollege
Status:	Pending approval by Management Committee
Category:	Statutory/Suggested
Review frequency:	Annualy
Contact:	**ICT Administrator or Head Teacher**
Version:	This policy has been adapted from the West Berkshire model
Who was consulted:	West Berkshire Council, ICT Administrator, Head Teacher, WBC School Improvement Adviser (IT & Strategic Education Business)
Other relevant policies:	Associated Policies: Safeguarding; Staff Conduct and Discipline; Data Protection, Wistleblowing Policy
Acronyms:	MC - Management Committee TLC - Teaching & Learning Committee SWC - Safeguarding & Wellbeing Committee FC – Finance Committee PERS - Personnel Committee LA - Local Authority WBC - West Berkshire Council HT - Headteacher SLT - Senior Leadership Team
Date for Review:	Autumn Term 2022

ICT & Online Safety Policy

ICT & Online Safety Policy

1: Key contact list for ICT & Online Safety Policy

Key contacts within the Local Authority Berkshire LSCB Procedures: http://berks.proceduresonline.com/			
Headteacher	Jacquie Davies	**01635 528048**	jdavies@icollege.org.uk
DSL	Faye Miller	**01635 48872**	Fmiller@icollege.org.uk
ICT Administrator and Online Safety Officer	Monica Romano	**01635 48872**	mromano@icollege.org.uk

2: Purpose	To ensure the effective and appropriate use of information and communications technology (ICT) & safe online use by and within icollege, this includes and is applicable to both staff paid or unpaid, volunteers and governors. The aim of this policy is not to impose unreasonable or unnecessary restrictions but rather to ensure that everyone accessing online media and using the ICT provided by icollege are supported to use it appropriately and within the current legislative framework and staff and children are safeguarded and protected from any misuse. The policy sets out the expectations of all members of the whole school community.
3: Roles and Responsibilities	All people (hereafter referred to as Users) using West Berkshire / icollege owned, or leased, ICT equipment, systems, or data whether this be from work, from home or from other location are responsible for complying with this policy and associated guidance. It is the responsibility of all adult ICT users to familiarise themselves with and to comply with this policy and the incorporated ICT User Usage Agreement. Compliance with this policy is a condition of working for icollege or using its ICT equipment or systems. All leaders and managers are directly responsible for implementing this policy and any related guidance and procedures within their service areas, and for the adherence of all users within their area. Everyone in the Service has the responsibility for handling protected and sensitive data in a safe and secure manner. **Governors** are responsible for the approval and work on the development of the policy, ensuring that it is implemented and review its effectiveness. In fulfilling this responsibility, the governing body delegates day to day responsibility to the Headteacher. The Governors will undertake the following regular activities: • Meetings with the online safety officer • Monitoring of online safety incident logs • Reporting to relevant governor committees annually or sooner if required • Keeping up to date with school Online Safety matters The **Headteacher** is responsible for ensuring the safety of members of the icollege' community, Day to day responsibility is delegated to the online safety officer. However, the Headteacher will ensure the following; • Staff receive suitable training enabling them to carry out online safety practices and support other colleagues as necessary

ICT & Online Safety Policy

	• There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff. The **Online Safety officer** is responsible for online safety issues and works with the relevant staff to review the policy and associated documents. The online safety officer will also ensure they liaise and develop positive working relationships with the Council's School Improvement service, school leaders, relevant governors and other school staff to ensure a culture of safeguarding, openness and transparency. To report any incident to the Headteacher and MC as required. The **Child Protection Officer/Leads** must be trained in online safety issues and be aware of child protection matters that may arise from any of the following: • Sharing of loss of personal data • Access to illegal/inappropriate materials • Inappropriate online contact with adults/strangers • Potential or actual incidents of grooming • Online bullying
4: Systems and data covered	ICT equipment, systems and data referred to in this policy include: - • Personal Computers (PCs) including desktops, laptops and tablets and associated peripherals such as printers, external drives etc. • Telephones and telephony equipment including fixed-line telephones, smart/mobile phones, VoIP 'soft' phones, 3G data cards and faxes • Any software application or database • Any system or server run applications • Other computer hardware including memory sticks, digital cameras • Social media sites including Instagram, Twitter, Facebook or similar

5: Use of ICT	**5.1 Appropriate use of ICT -** It is the policy of iCollege to ensure that its ICT equipment, systems and data are used effectively and efficiently for the needs of it's Services and are not misused. The staff and governors have a duty to protect the availability, integrity and security of ICT equipment, systems and data within its use. This is to be done following the guidance outlined in this document and any additional more detailed guidance as may be issued from time to time.
	
	All users must ensure that to the best of their abilities they:-
	• use ICT only for lawful activities (in accordance with United Kingdom and International law).
	• take reasonable measures to safeguard the physical security of ICT related equipment and data they use.
	• Comply with the Council's Financial Regulations regarding procurement and control of ICT assets.
	• take reasonable measures to prevent unauthorised access to systems and information used. These measures will include, but are not limited to:
	  ○ safeguarding passwords/phrases
	  ○ not letting others use equipment, or access systems or accounts assigned to them
	  ○ not removing security measures, or allowing others to do so
	  ○ logging out of, or locking systems when they are left unattended, particularly when non-filtering option (staff proxy) is engaged on the

ICT & Online Safety Policy

computer
    - No sensitive data is to be extracted from ICT systems to any other media eg: removable disks, memory sticks, shared drives unless absolutly necessary and with permission of the ICT administrator
    - safeguarding printed information extracted from systems
    - not sending sensitive data outside of the organisation except when using approved secure means
    - when using a free wi-fi link, colleagues must ensure that the link is secure. Check Google for current info on how to do this
- abide by the rules of the ICT User Usage Agreement.

5.2 Misuse of ICT
Users of icollege facilities shall not -

- use ICT to engage in any criminal activity
- use ICT to access or distribute any unsuitable materials (e.g. racist, pornographic, media promoting violence etc.)
- wilfully try to access systems or information for which they are not authorised, or to assist others to do so
- fraudulently use or access any system or information, or fraudulently amend any records
- use the icollege systems for their own business purposes, or for monetary gain
- knowingly infringe copyright laws
- switch off, bypass or ignore security controls or restrictions
- make inappropriate or excessive use of icollege systems for private or non-council use.
- Staff should be aware of how to complain and when to complain or report any suspicious or inappropriate behaviour that they may witness or find in the use of ICT/Online access, see also the icollege Whistleblowing Policy

5.3 Privacy
The icollege along with West Berkshire Council provides ICT facilities for the effective sharing of information between employees and its external suppliers, partners and customers. These facilities are provided to support the business and as such any information created or input to these systems (e.g. email messages) are and remain the property of the icollege.

Such information is not the private property of any individual nor shall any individual expect there to be any personal privacy with respect to any such information, whether it be designated “private” or not.

Whilst not routinely monitoring an individual’s use of ICT the icollege maintains the right to review, audit, intercept, access, monitor, delete or disclose any information, created, sent, received or stored on its ICT systems for any purpose.

In so far as is allowed by the Human Rights Act, managers may request access to information produced (e.g. emails) by staff within their service, or request usage statistics on individuals (e.g. for time spent on the internet, sites visited, phone calls made etc.). Such a request would be authorised by the Head Teacher and would normally be conducted by the Council. **See Appendix 12.5**

5.4 Failure to comply with the icollege Policy
This document together with the ICT User Usage Agreement and other relevant published standards and procedures provides ICT users with essential information regarding the acceptable use of ICT in the Services and sets out conditions to be followed. It is the responsibility of all to whom this

ICT & Online Safety Policy

	policy applies to adhere to these conditions. Failure to do so may result in; • withdrawal of access to relevant services • informal disciplinary processes • formal disciplinary action (in accordance with the Council's schools disciplinary procedure. Additionally, if a criminal offence is suspected the icollege or Council may contact the police or other appropriate enforcement authority to investigate.
6: Good Practice	**All users of icollege shall:-** • Safeguard access by protecting passwords • In general, Temporary passwords will be created for you. **See Appendix 12.4** You will be asked to change your password on your first login. Please ensure you will: o create and use passwords that are not easy to guess or crack o use passwords with a minimum length of 8 characters containing both upper and lower case letters and at least one numerical digit o not use names, or dictionary words (16 digit passwords offer maximum security) o avoid details personal to you that might be known e.g. spouse's name, birthday, etc. o keep passwords confidential o avoid keeping a paper record of passwords • only store information and files in approved 'safe' locations e.g. on share point. • No sensitive or personal data should be stored on One Drive [One Drive is a personal cloud storage option that allows users to store files that can be accessed from a web browser or a mobile device, as well as shared publicly or with specific people, allowing users to upload, create, edit and share Word, Excel, PowerPoint and OneNote documents directly within a web browser.] • **DO NOT** store files on 'local' drives i.e. the hard drive C: drive of a desktop or laptop PC. Where files are stored locally staff must take responsibility for the security of the information and for creating backups. • **DO NOT** copy sensitive information on 'local' storage such as memory sticks, or CDs due to the risk of the data being lost or stolen. • perform regular housekeeping on computer records and information (e.g. by deleting files and emails etc. no longer required). • ensure that you have received the appropriate training to use the equipment and software safely and effectively. • report faults, especially those that might compromise data security or integrity, to the person responsible for IT in the service in a timely manner. • report actual or suspected security leaks or breaches, equipment or information loss to the line manager or person responsible for IT and then the Head teacher as soon as a proven breach has occurred.
7: Use of the	**7.1** The Service understands that the Internet is very useful for quickly and easily accessing and researching information and keeping up-to-date with news and

ICT & Online Safety Policy

Internet	professional development, etc. Government departments and professional bodies have websites which contain information which is vital to many of us to carry out our jobs effectively. It is therefore an essential tool provided to users. The icollege also recognises that users may, from time to time, need to access the Internet for personal reasons. This should not however take place during the working day. Users are therefore allowed to access non-work sites within reasonable limits in accordance with the following code of practice: • Students and staff will be informed that internet access will be monitored • The icollege will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Icollege cannot accept liability for the material accessed, or any consequences of internet access. • Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive. • Users must not attempt to disable or reconfigure any filtering, virus protection or similar. • All students using the internet, and associated communication technologies, will be made aware of the school's Online Safety Guidelines. • Students will receive guidance in responsible and safe use on a regular basis. **From September 2020, Relationships Education will be compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England.** **Through these new subjects, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives. This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly,respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.** **Government Guide on Teaching Online Safety in School** **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf** **DO NOT** use the Internet, in normal circumstances, to access websites other than for work purposes during core working hours, except with the permission of your line manager. There may be some websites (e.g. travel news) which you may legitimately need to access during core working hours to get important information which will affect your work-life balance. If you need to do this, you should restrict the time spent on the website to no more than a few minutes. If you are in any doubt

	about accessing non-work-related websites during the working day, you should discuss this with your line manager. **DO NOT** use the Internet to access or update your own personal social networking websites (e.g. Facebook) or to access any other recreational sites during core working hours, as doing so means that you are wasting time for which staff are being paid. However, you may need to use the above to support students to use their social networking sites appropriately. ***It is important that access to the Internet is used responsibly and legally. Users must not take any action which could bring the icollege into disrepute, cause offence, interfere with individual's or the organisation's work or jeopardise the security of the icollege's systems, software or data.*** **7.2 Internet Filtering** – The icollege uses internet filtering on their machines. This is currently provided through RM Safety Net. The filtering system is configured to block access to sites containing offensive, illicit or potentially dangerous information including, pornographic material, racial hatred or religious hatred, or other discrimination or hatred, sites involving or promoting violence or illegal acts. The filtering system also protects against potentially harmful files such as computer viruses by preventing the download of certain types of files. Other sites such as gambling, file sharing sites etc. are also blocked. **DO NOT** attempt at any time to access websites in any of these blocked categories. Users must be aware that no protection system is 100% guaranteed and that they may still inadvertently gain access to unacceptable, offensive or other normally blocked materials. People inadvertently accessing offensive material when accessing the Internet should inform the person responsible for IT who can make appropriate decision to inform the RM SafetyNet Help Desk to alter the filter immediately. Accidental access will not normally result in any disciplinary action but failure to report it may do so. Users shall not attempt to download or install unauthorised software from the internet. Users should be aware that, as with other information sources, not all information on the Internet is accurate, complete or reliable. Users should independently ensure its validity, and their rights to use it, before making use of it for icollege business. Staff shall not bypass the procurement procedures by buying items for the icollege over the Internet. There may be occasions where purchasing items over the internet is the only, or best option. In these cases users should obtain the authority of the Headteacher and use the appropriate method of procurement.
8: Use of Email	**Email is now a primary form of communication -** The email system now provides the facility to send secure email ([secure]) This functionality should always be used when sending sensitive or confidential information by email, particularly where it is been sent to an external email address. An email message will have the same legal status as any other written document and must therefore be treated in the same way

ICT & Online Safety Policy

as any other formal business correspondence.

Icollege email users should conform to the following code of practice:-

- **DO** use meaningful subject title to help the recipient gauge the relevance and importance of each email they receive.
- DO NOT include a name in the subject title
- **DO** check spelling and grammar as you would other written communications
- **DO** check emails regularly and delete old or unwanted emails in your mailbox
- **DO** implement an out-of-office rule or provide delegated access to your email when you will be away from the office for an extended period to ensure no important messages are ignored or delayed
- **DO NOT** send any emails which are unlawful or which breach any icollege standards or policies or are not aligned with the icollege values. This includes messages that may harass or offend someone. Harassment can take the form of argumentative or insulting messages or any other message that the sender knows or, or might reasonably be expected to know, would cause distress to a recipient.
- **DO NOT** breach privacy by forwarding information known to be confidential or data sensitive, or likely to upset or offend the recipient without the consent of the original sender.
- **DO NOT** send emails from someone else's account, except under proper delegated arrangements where individual accountability is retained, as this may constitute impersonation or misrepresentation of another individual.
- **DO NOT** send emails from non-corporate accounts e.g. hotmail, yahoo etc. containing official icollege business. These accounts are outside of the control of the icollege and are not secure.
- **DO NOT** copy people in to emails unless considered essential and do not reply to all when a reply to sender will suffice.
- **DO** check when forwarding emails the content of all previous emails as you might be passing on information not intended for that recipient
- **DO** ensure that you have completed a signature box on your email to include your role and contact details.
- Students may only use approved e-mail or message accounts on the school system.
- Students must be advised and supported to immediately tell a staff member if they receive an offensive e-mail or message.
- Students must be advised and supported not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an email or message.
- Students wishing to send e-mails to an external person or organisation must be

ICT & Online Safety Policy

	authorised by a member of staff before sending.
9: Social Networking	For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, Instagram, Google+, Pinterest, Tumblr, Reddit, Snapchat, Secret, YouTube, Skype, Second Life, LinkedIn, WhatsApp, Vine, WeChat, Kik, blogs, chat rooms and online gaming etc. • Staff have a perfect right to use social networking sites in their private life. In doing so they must ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity. • Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff. • The use of social networking 'tools', e.g. blogs, wikis, messaging, etc., within the school environment is both acceptable and to be encouraged. [See the Social Networking Responsibilities Guidance for further information available on Share Point]
10: Use of Telephones Tele communication Equipment and Portable Equipment	This section covers the use of icollege telephones/telephony equipment that includes fixed (desk) phones and icollege purchased mobile phones including smart phones. Some policies are applicable to all phone types whereas others, are applicable only to a particular phone type e.g. mobile phones. **10.1 General** Users should not try to bypass any security measures or cost controls in place on their telephony equipment without prior consent from their line manager. icollege telephony equipment is provided to help users engaged on Service business conduct their daily work. Personal use of this equipment should be avoided and where personal usage is deemed excessive by the icollege, users may be asked to reimburse costs incurred. Users shall answer their telephone in polite and professional manner and uphold the values and the ethos of the icollege. Where voicemail is used it must not be viewed as an alternative to answering the telephone and voice mailboxes must be checked on a daily basis. **10.2 Desk Phones** Desk phones should not be plugged or unplugged from the network without prior approval. Desk phone telephone usage is controlled and phone bills are scrutinised and compared to identify any inappropriate usage**.** **10.3 Mobile Phones** icollege mobile phone users should not loan or reallocate their phone or SIM card to anyone else without the prior knowledge and approval of their line manager. Mobile phone telephone usage for contract phones is controlled i.e. users cannot dial premium rate or international number, and monitored to track call destinations, duration and costs. Pay as you go phones are monitored by use of top up costs.

ICT & Online Safety Policy

	Mobile phones (contract) - users must protect these with a PIN or other security access. Mobile phone users should not let anyone use their mobile phone to make telephone calls (except other icollege users in special circumstances). Responsibility for calls made from an allocated phone rests with the nominated user and any misuse will also be their responsibility. icollege staff should never use their mobile phones whilst driving. Any phones that are used for work purposes, particularly those that send or receive email, should be locked with a pin code/password for safeguarding purposes. This applies equally to icollege owned phones and staff personal phones. **10.4 Use of Portable Equipment** All guidelines in this policy apply equally to portable equipment as to fixed equipment. However portable equipment is more vulnerable to certain types of misuse, and to theft. **Staff issued with laptops will be required to sign the equipment loan form and confirmed they have read this policy.** Portable equipment includes: Smart/Mobile Phones, 3G/4G Data Cards, Personal Data Assistants (PDAs), Laptop PCs, Tablet PCs, Memory sticks, Digital Cameras etc **Users issued with portable equipment should take all reasonable steps to safeguard the security and physical protection of these items by following the guidelines below:** • When transporting portable equipment use approved protection e.g. laptop bag or backpack • To prevent theft of portable equipment do not leave unattended; do not leave visible in vehicles; use locks where possible • Apply timeout password on any devices where these are available • In the case of Laptop or Tablet PCs only use supplied equipment with an encrypted hard drive or encrypted memory stick/portable hard drive. • avoid saving data onto the local hard drive 'C: Drive'. Staff can save any documents on the ONE Drive [personal cloud] in their icollege email account. • ensure that the lap top has appropriate and updated Sophos anti-virus protection • Report thefts or suspected misuse immediately to the SBM/Unit Lead Teacher/Pastoral Manager and person responsible for IT • Portable equipment should be included in the insurance. **See Appendix 12.6 for Acceptable Use template forms**
11: Control of ICT Assets (Hardware and	**11.1 Inventory - The icollege maintains an inventory of the ICT hardware and software. Each ICT asset is recorded for the purposes of:** • security protection

ICT & Online Safety Policy

Software)	• insurance • financial asset management • health and safety • equipment maintenance and replacement • software licence compliance No equipment or software should be acquired, disposed or relocated without the prior knowledge and approval of the person responsible for IT. Line managers are responsible for retrieving icollege ICT equipment from staff when they leave and ensuring that the inventory is updated by informing their admin staff. **11.2 Backup and disaster recovery plan** The Headteacher with the support of the WBC IT department and the icollege ICT administrator will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime includes: • The use of a remote location for backup of key school information. • No data should be stored on the C drive of any curriculum computer as it is liable to be removed without notice during routine maintenance. Staff are responsible for backing up their own data on teacher laptops/devices and should utilise the method currently recommended. At present this is manual copying of files to the user's individual 'U' drive on the school server. This will be backed up each evening and can be restored from the date of the backup. It is recognised that some staff are not able to make regular copies of data to the server. **11.3 Software** Purchased software should be checked for educational suitability by Lead teachers and team leaders. • Staff should not load software onto any machine without permission. • Networked software will be uploaded by education IT. Please request this via the IT log which is SharePoint **11.4 Digital and video images** **Parental permission** • icollege will ensure that appropriate written permissions are obtained before taking and use of digital and video images of students. Such use could include icolleges website; social media (Twitter); display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press. • Parental permission is to be obtained annually. • Students will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online. • Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded. **Storage and deletion** • All images of students will be securely stored in one central location. • Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then

be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.
- Digital images may be retained for up to 2 years after a pupil has left the school and are then deleted in line with the data retention policy.

Recording of images
- All staff and students must sign the relevant Acceptable Use Agreement.
- School digital devices should always be used to record images of students.
- All students appearing in images should be appropriately dressed.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Where images are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online 'cloud' storage) care must be taken that the location of images of students is clearly understood and in line with ICO (Information Commission's Office) guidance.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to icollege or personal, may be subject to scrutiny if required.
- Where volunteers are supporting icollege staff, they should advised and supported to abide by the same rules.

Use of staff personal devices
Staff personally owned devices (e.g. staff smartphones, cameras, tablets) must not be used to record images, video or voice.

Parents taking photographs or video
Where icollege chooses to allow the recording of images at 'public' events the following should apply:
- Images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

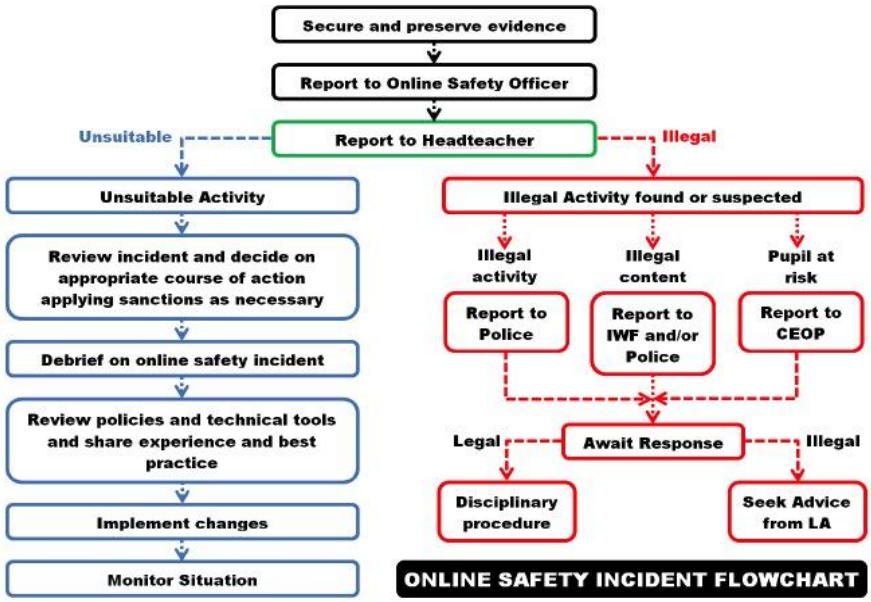
Events/Activities involving multiple schools
- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
- Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although icollege will make reasonable efforts to safeguard the digital images of students, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The icollege cannot therefore be held accountable for the use of images taken by parents or members of the public at events. (See Appendix 12.6 Acceptable Us Agreement forms - Use of Digital/Video Images Agreement)

11.5 Icollege website
- The icollege website should include the icolleges addresses, icollege e-mail, and telephone including any emergency contact details.
- The website will be used to provide information and guidance to parents concerning online safety policies and practice.
- Staff or students' home information will never be published.
- The copyright of all material posted will be held by icollege and be clearly attributed to the owner where permission to reproduce has been obtained or

ICT & Online Safety Policy

	given e.g. via Creative Commons licensing.
12: Appendices	
12.1 School and the Data Protection Act	***General Data Protection Regulations in May 2018*** iCollege processes personal data, including sensitive personal data, relating to Pupils, Parent/ Carers/ Staff, service Providers governors and volunteers in the course of engagement with the school. For these purposes, we (the school) will act as the Data Controller, pursuant to the General Data Protection Regulations (GDPR). The privacy notices for Staff and Pupils are published on iCollege Website and SharePoint. These notices explain how and why we collect personal information what we do with that information. We are committed to protecting personal information in line with the UK privacy legislation. The icollege has the appropriate level of security to prevent the personal data held (e.g. for staff, students and parents) being accidentally or deliberately compromised.
12.2 Course of action if inappropriate content is found	If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user must: • Keep the computer on and turn off the monitor or minimise the window. • Report the incident to the teacher or responsible adult. The teacher/responsible adult must: • Ensure the well-being of the pupil. • Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the students). • Report the details of the incident to the Online Safety Officer. • It is advisable to copy and paste the web page address and send it to the Online Safety Officer. The Online Safety Officer will then: • Log the incident and take any appropriate action. • Where necessary report the incident to the IT Technician and Internet Service Provider so that additional actions can be taken. **Online Safety Flowchart**

ICT & Online Safety Policy



12.3 Online Safety Log	**The Online Safety Incident Log and Form is to be completed in the presence of the Online Safety Officer.**

Date/time of incident	Date/time incident logged	Name person completing log	Description of incident (eg nature of incident, where it occurred who was involved)	Follow up Actions

Signature: **Write name:**

Online Safety Officer:
Signature: **Write name:**

12.4 Password guidance	This guidance is intended for those adults using school systems but is based on good practice and should also feature in the teaching of, and advice to, students. Passwords must have a 'strength' of at least 12 characters where a letter is 1unit and a number or punctuation mark is 2 units. The choice of password 'strength' should be appropriate to the data being protected and the potential risks associated

	with that data being compromised. Passwords should avoid following a pattern or being predictable. Passwords must not be easily guessable by anyone and therefore should not include: • Names of family, friends, relations, pets etc. • Addresses or postcodes of same • Birthdays • Telephone numbers • Car registration numbers • Unadulterated whole words Try to use in a password: • A mixture of letters and numbers • Punctuation marks • At least 8 characters Think of a memorable phrase such as the example below to construct a password: **R**un, **r**un **a**s **f**ast **a**s **y**ou **c**an **– Y**ou **c**an't **c**atch **m**e, **I**'m **t**he **G**ingerbread **M**an**!** A password can be constructed by using the first letter of each word and changing some letters to their digit equivalent. Password: Rrafayc-Yccm1tGM! • Use a password strength checker such as https://howsecureismypassword.net/ It would take a computer about 93 trillion years to crack the above password.
12.5 Sensitive & Non-sensitive data	**Sensitive data will include:** • SEN records such as IEPs and Annual Review records • Mark sheets and assessments • Reports and Open Evening comments • Personal data stored on the school's Management Information System, e.g. SIMS • Photographic or video material • Name, address and contact information **Non-sensitive data thus includes:** • General teaching plans • Curriculum materials • General correspondence of a non-personal nature
12.6 Acceptable Use Agreements	
Foundation and Year 1 Pupil	**Nursery, Foundation and Year 1 Pupil Acceptable Use Agreement** **This is how we stay safe when we use computers:**

ICT & Online Safety Policy

Acceptable Use Agreement	• I will ask a teacher or suitable adult if I want to use the computers. • I will only use activities that a teacher or suitable adult has told or allowed me to use. • I will ask permission before I use the internet. • I will take care of the computer and other equipment. • I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong. • I will tell a teacher or suitable adult if I see something that upsets me on the screen. • I know that if I break the rules I might not be allowed to use a computer. I have read the agreement with my child and they have understood the above and agree to follow the rules outlined. **Unit Name:** **Pupil Name:** **Parent Signature:** **Date:**
Years 2 and 3 Pupil Acceptable Use Agreement	**Years 2 and 3 Pupil Acceptable Use Agreement** **For my own personal safety:** • I understand that the school will check that I am using my computer sensibly. • I will keep my username or password private. • I will keep information about myself or anyone else private when online. • I will not arrange to meet people that I have communicated with online. • I will report anything that makes me feel uncomfortable when I see it online. **Respecting everyone's rights to use technology as a resource:** • I understand that the school ICT systems are for learning and that I will only use them for playing games when I have permission to do so. **Acting as I expect others to act toward me:** • I will respect others' work and will not change, copy or remove other user's files. • I will be polite and responsible when I communicate with others. • I will only take or share images of anyone with their permission. **Keeping secure and safe when using technology in school:** • I will only use school's ICT equipment when given permission. • I will not upload, download, or access any material that I am not supposed to. • I will immediately report any damage or faults. • I will keep the computer settings as they are. • I will immediately tell a staff member if I receive offensive messages. **Using the internet for research or recreation:** • I will only use the work of others when given permission (including music and videos).

ICT & Online Safety Policy

	Taking responsibility for my actions, both in and out of school: • I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet. I have read/had read to me the above and understand and agree to follow the rules outlined. **Unit Name:** **Pupil Name:** **Parent Signature:** **Date:**
Years 4, 5 and 6 Pupil Acceptable Use Agreement	For my own personal safety: • I understand that the school will monitor my use of the ICT systems, messages, and other digital communications. • I will keep my username or password private and only use my own when logging into an account. • I will keep information about myself or anyone else private when online (e.g. home address and telephone number). • I will not arrange to meet people that I have communicated with online. • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online. Respecting everyone's rights to use technology as a resource: • I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal or recreational use. • Permission must be given before the school ICT systems can be used for social media, gaming or file sharing. • I will keep my downloads and uploads to a minimum unless I have permission. • I will not use the school ICT systems for online gambling or internet shopping. Acting 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 only take or share images of anyone with their permission. Keeping secure and safe when using technology in school: • I will only use approved ICT Equipment on the school system. • Permission must be given before I bring and use my personal handheld/external devices into school (e.g. Laptops, Tablets, USB devices, etc.). • I will hand my mobile phone over to staff at the beginning of the day and it will be returned to me before I go home. The mobile phone must be switched off before I enter the school and can be turned on after I exit the school. • I will not 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. • I will keep the computer settings as they are and not load software or

ICT & Online Safety Policy

	applications. • I will immediately tell a staff member if I receive any offensive messages. Using the internet for research or recreation: • When I am using the internet to find information, I should take care to check that the information that I access is accurate. • 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 download copies (including music and videos). Taking responsibility for my actions, both in and out of school: • I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (e.g. online bullying, inappropriate use of images and/or personal information). • I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet. I have read and understood the above and agree to follow the rules outlined. Unit Name: Pupil Name: Parent Signature: Date:
Parent/Carer Acceptable Use Agreement **Use of Digital/Video Images Agreement**	The school seeks to ensure that students have good access to ICT to enhance their learning and, in return, expects students to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the students 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. Parent/Carer's Name: Pupil's Name: Unit Name: As the parent/carer of the above pupil, I understand that my son/daughter will have access to the internet and to ICT systems at school. I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of ICT – both in and out of school. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that students 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, as no filtering system is 100% safe. 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.

ICT & Online Safety 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 online safety. I have read the Pupil Acceptable Use Agreement attached and agree that my child will abide by the rules. Parent/Carer's Name: Pupil's Name: Unit Name: Use of Digital/Video Images Agreement 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, the school's Twitter account 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 students cannot be identified by the use of their names. In accordance with guidance from the Information Commissioner's Office, parents/carers may be allowed to take videos and digital images of their children at school events at the school's discretion for their own personal use (as such use in 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 and for the parents/carers to agree. Parent/Carer's Name: Pupil's Name: Unit Name: As the parent/carer of the above pupil: • I agree to the school taking and using digital/video images of my child. 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 such as their publication in newsletters, on the school website and occasionally in the public media. Yes / No • I agree to the school using the digital/video images of my child on the school's Twitter account. 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 the above guidelines in my use of these images. Parent/Carer's Name: Pupil's Name: Unit Name:

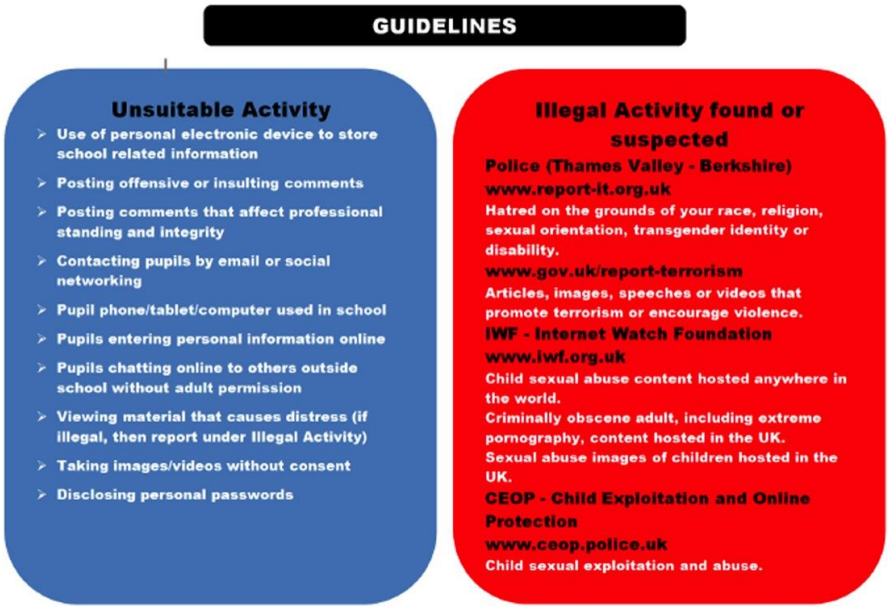
ICT & Online Safety Policy

Laptop/Devices Acceptable Use Agreement	**1. Introduction** • This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school. • It should be read in conjunction with the school's Online Safety Policy. • All recipients and users of these devices should read and sign the agreement. **2. Security of equipment and data** • The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft, or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss. • Laptops and other associated devices should never be left unattended in a vehicle at any time. Staff will be responsible for any loss in the event of theft or damage in this event. • Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled. **3. Software** • Staff will not load onto any device additional software without the assistance of the ICT Administrator • Any such software should be in connection with the work of the school. No personal software should be loaded. • Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties. • Users should not attempt to make changes to the software and settings that might adversely affect its use. **4. Faults** • In the event of a problem with the computer, the school's ICT Administrator should be contacted. • Do not attempt repairs – this will invalidate any warranty on the equipment. **Declaration:** I have read and understood the above and also the school's Online Safety Policy and agree to abide by the rules and requirements outlined. **Name:** **Signature:** **Date:**
Staff Acceptable Use Agreement **Code of conduct**	To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should always refer to this policy for clarification and guidance and all associated policies. • I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. • I appreciate that ICT includes a wide range of systems, including mobile phones,

ICT & Online Safety Policy

	PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business. • I understand that school information systems may not be used for private purposes without specific permission from the Headteacher. • I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance. • I will respect system security and I will not disclose any password or security information to anyone other than the IT Technician. • I will not install any software or hardware unless authorised, e.g. on a school laptop. • I will ensure that personal data, particularly that of students, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety Policy. • I will respect copyright and intellectual property rights. • I will ensure that electronic communications with students (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. • I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. • I will ensure that pupil use of the internet is consistent with the school's Online Safety Policy. • When working with students, I will closely monitor and scrutinise what students are accessing on the internet including checking the history of pages when necessary. • I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing. • I know what to do if offensive or inappropriate materials are found on screen or printer. • I will report any incidents of concern regarding students' safety to the appropriate person, e.g. Online Safety Officer and/or SLT member. The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds. **Name:** **Signature:** **Date:**

ICT & Online Safety Policy

12.7 Unsuitable / Inappropriate activities	
Safeguarding and remote education during coronavirus (COVID-19)	Where a class, group or small number of pupils need to self-isolate, or there are local restrictions requiring pupils to remain at home, the Department for Education expects schools to be able to immediately offer them access to remote education. Schools should ensure remote education, where needed, is safe, high quality and aligns as closely as possible with in-school provision. iCollege will continue to improve the quality of remote education and have a strong contingency plan in place for remote provision. Keeping pupils and teachers safe during remote education is essential. Teachers delivering remote education online should be aware that the same principles set out in the school's code of conduct will apply. iCollege has updated the policies to reflect remote online education. Resources to understand more about how to ensure online education is safe: • Remote education advice from The Key for School Leaders • Advice from NSPCC on undertaking remote education safely • Guidance from the UK Safer Internet Centre on remote education Schools can access the free Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm. Guidance on teaching online safety in schools provides information to help schools ensure their pupils understand how to stay safe and behave online. Full Guidance: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

ICT & Online Safety Policy

13: Associated policies and information	Staff Code of Conduct Data Protection Safeguarding and Child Protection Policy Social Networking Responsibilities Guidance
14: Change Record	

Keeping Children Safe in Education September 2020

All staff with the iCollege take seriously their responsibility to protect and safeguard the welfare of children and young people in their care; this includes protecting children from maltreatment; preventing impairment of children's Mental and Physical health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.

Version Number	Date Approved	Management Committee Minute Reference	Description of Amendments	Date
V3	08/08/13, July 2015	RMUnify / School site / Staff handbook	Original Version July 2011 SW (developed from WBC corporate ICT policy) update July 2015	
V4	MC 30.11.17	MC minutes 30.11.17	Complete re-write	Sept 2017
V5			Sensitive data storage clarifications	October 2019

Approved by:	Management Committee
	December 2020
Review date:	
	December 2021

Keeping Children Safe in Education 2020

*All staff with the **iCollege** understand the need to safeguard and promote the welfare of children; this includes protecting children from maltreatment; peer-pressure; preventing impairment of children's health or development; ensuring that children grow up in circumstances with the provision of safe and effective care; and taking action to enable all children to have the best outcomes. Children includes everyone under the age of 18*