



iCollege

Alternative Education West Berkshire

ICT (Information & Communication Technologies)

& Online Safety Policy

Document Control	
Document Name	ICT (Information & Communication Technologies) and Online safety Policy
Category:	Statutory
Date:	Feb 26
Version:	4.3
Written by:	MR, amended by FM
Associated policies and useful information	AI policy Staff Code of Conduct Data Protection Safeguarding and Child Protection Policy Social Networking Responsibilities Guidance https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime
Review:	Annually
Status	APPROVED

Contents

1 Key contacts :	2
2: Purpose	3
3: Roles and Responsibilities.....	3
4: Systems and data covered	4
5: Use of ICT.....	4
5.1 Appropriate use of ICT	4
5.2 Misuse of ICT	4
5.3 Privacy	5
5.4 Failure to comply with the iCollege Policy	5

INSPIRATION KS1 & 2 Foxglove
Way,
Thatcham, Berkshire,
RG18 4DH
01635 877114

POD PLUS KS3
Modular Building
Paynesdown Road,
Thatcham, Berkshire,
RG19 3TE
01635 243208

**The POD KS2
INTERVENTION KS3 & 4**
88 Newtown Road,
Newbury, Berkshire,
RG14 7BT
01635 49397

INTEGRATION KS3 & 4
22, Highview, Calcot,
Reading, Berkshire,
RG31 4XD
01189 416636

INDEPENDENCE KS4 & 5
Richmond House, Bath Road,
Newbury, Berkshire,
RG30 1QY
01635 48872

6: Good Practice	5
7: Use of the Internet	6
7.1 Internet access.....	6
7.2 Internet Filtering	7
8: Use of Email	7
9: Social Networking	8
10: Use of Telephones Tele communication Equipment and Portable Equipment	8
10.1 General	8
10.2 Desk Phones.....	9
10.3 Mobile Phones	9
10.4 Use of Portable Equipment	9
11: Control of ICT Assets (Hardware and Software).....	9
11.1 Inventory	9
11.2 Backup and disaster recovery plan	10
11.3 Software.....	10
11.4 Digital and video images	10
11.5 ICollege website.....	11
12: Appendices	11
12.1 School and the Data Protection Act	11
12.2 Course of action if inappropriate content is found	12
12.3 Online Safety Log	13
12.4 Password guidance	14
12.5 Sensitive & Non-sensitive data	14
12.6 Fair processing notice.....	15
12.7: Staff Acceptable Use Agreement Code of conduct.....	16
12.8 Unsuitable / Inappropriate activities	17

1.Key contacts	Berkshire West Safeguarding Children Partnership http://berks.proceduresonline.com/reading/index.html		
Headteacher iCollege	Jacqueline Davies	01635 528048	jdavies@icollege.org.uk
DSL and online safety officer	Faye Miller	07771989791	DSL@icollege.org.uk fmiller@icollege.org.uk
School Business Manager (SBM)	Karen Price	01635 48872	kprice@icollege.org.uk

School Improvement Adviser [IT & Strategic Education]& LA Data protection officer	Gerard Strong	07500 785950	Gerard.Strong1@westberks.gov.uk
--	---------------	--------------	--

2: Purpose

This policy provides guidelines 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.

This policy sets out the expectations of all members of the iCollege 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 and the Headteacher will ensure iCollege has appropriate filtering and monitoring systems in place and regularly review their effectiveness (at least annually).

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 DSL and 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 DSL and 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

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 **DSL/Online Safety officer** is responsible for online safety issues and works with the relevant staff to review the policy and associated documents. They 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. They will report any incident to the Headteacher and MC as required.

The **Designated Safeguarding Lead (DSL)** will take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

ALL staff should report any concerning online activity/access in-line with iCollege safeguarding procedures and using the on-line reporting system (Safeguard My School).

4: Systems and data covered

ICT equipment, systems and data referred to in this policy include:

- Personal Computers (PCs) including desktops, laptops, 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 the 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 computer
 - avoiding copying any sensitive data extracted from ICT systems to other media e.g. removable disks, memory sticks, shared drives unless they are encrypted.
 - 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, also refer to 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 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, passwords will be created for you. See Appendix 12.4

In situations where you have to create your own password then;

- create and use passwords that are not easy to guess or crack
 - use passwords with a minimum length of 8 characters containing both upper and lower case letters and at least one numerical digit
 - not use names, or dictionary words (16 digit passwords offer maximum security)
 - avoid details personal to you that might be known e.g. spouse's name, birthday, etc.
 - keep passwords confidential
 - avoid keeping a paper record of passwords
- only store information and files in approved 'safe' locations e.g. on the One Drive.

[One Drive 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, U: 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 unencrypted 'local' storage such as unencrypted memory sticks 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 Internet

7.1 Internet access

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 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.

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:-

- Learners and staff will be informed that internet access will be monitored
- 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 learners using the internet, and associated communication technologies, will be made aware of the school's Online Safety Guidelines.
- Learners will receive guidance in responsible and safe use on a regular basis.

DO NOT use the Internet, 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 learners 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

iCollege uses internet filtering on their machines. This is currently provided through RM Unify.

RM SafetyNet supports iCollege's online safeguarding policies and the implementation of a balanced curriculum.

By default, illegal websites are blocked by RM SafetyNet based on input from the Internet Watch Foundation, the Home Office, the Counter Terrorist list and security intelligence, including radicalisation content.

DO NOT attempt at any time to access websites in any of these blocked categories.

The technology safeguards devices brought into school when they're connected to the network:

- Web filtering to prevent users from accessing inappropriate material in a school environment
- Alerts can be set up to notify the Administrator of attempted access to harmful or sensitive content, highlighting any non-compliant browsing activity
- As a result reports on an individual's web browsing activity can be obtained for investigation, either for their own protection or the school's, as required by the DfE guidance, KCSiE

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 DSL/online safety officer 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/School business manager and use the appropriate method of procurement.

8: Use of Email

Email is a primary form of communication - The email system 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 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 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, GMail 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 NOT set auto-forward iCollege emails to private email account or other iCollege email accounts
- DO ensure that you have completed a signature box on your email to include your role and contact details.
- Learners are not currently offered an e-mail account on the school system.

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 iCollege website > Statutory information> Policies]

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 the School business manager .

Mobile phone telephone usage for contract phones is controlled i.e. users cannot dial premium rate or international numbers, and it is monitored to track call destinations, duration and costs. Pay as you go phones are monitored by use of top up costs.

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 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/5G 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'/ U: Drive. Staff can save any documents on the ONE Drive [personal cloud] in their iCollege email account.
- ensure that the laptop has appropriate and updated Sophos anti-virus protection
- report thefts or suspected misuse immediately to the SBM

See Appendix 12.6 for Acceptable Use template forms

11: Control of ICT Assets (Hardware and Software)

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

- 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 SharePoint or One Drive. This will be backed up each evening and can be restored for 2-3 months from the date of the backup.

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 the ICT Coordinator or MIS
Please request this via the IT log on 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 learners.
Such use could include iCollege website; social media (Twitter/ Facebook); 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.
- Learners 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 learners 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 learners must sign the relevant Acceptable Use Agreement.
- School digital devices should always be used to record images of learners.
- All learners appearing in images should be appropriately dressed.
- Learners 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 learners 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 be 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 learners, 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 Use Agreement forms - Use of Digital/Video Images Agreement)

11.5 iCollege website

- The iCollege website should include the iCollege's 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 learners' 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 given e.g. via Creative Commons licensing.

12: Appendices

12.1 School and the Data Protection Act

'UK GDPR' sits alongside an amended version of the DPA 2018.

Working toward UK GDPR compliance:

UK GDPR requires schools to be more accountable for the information they collect. Therefore, all actions that do not comply with usual school procedures will require a student's full consent, particularly if data is handled by a third party.

Right to be informed

Schools must ensure all staff and learners are aware of UK GDPR, how data is collected and stored and the implications of a breach.

Right to give consent

Schools should have systems in place that gather parental consent for data processing and also verify individuals' ages.

Right to know where your data is stored

The school must provide visibility on what software is being used for teaching and data collection, such as teaching apps.

Right to rectification

The school must give the student the ability to request changes to his or her personal data if he or she believes it is out of date or inaccurate.

Right to erasure/right to be forgotten

The school must give the student the ability to ask for the deletion of their data. This will generally apply to situations where the student's relationship has ended with the school.

Right to restrict processing

A student can exercise this privilege to request that his or her request (for example, a loan request) be examined personally because he or she believes that automatic processing of his or her loan will not take into account the learners individual situation

Right to data portability

The school must allow the student to request that his or her personal data be relocated. The student may request that his or her personal data be returned (to him or her) or transferred to another controller as part of such a request.

Additionally, because schools are considered public authorities under UK GDPR, they are obligated by law to hire or appoint a Data Protection Officer.

The iCollege has the appropriate level of security to prevent the personal data held (e.g. for staff, learners 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 illegal, pornographic, violent, sexist or racist) 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.

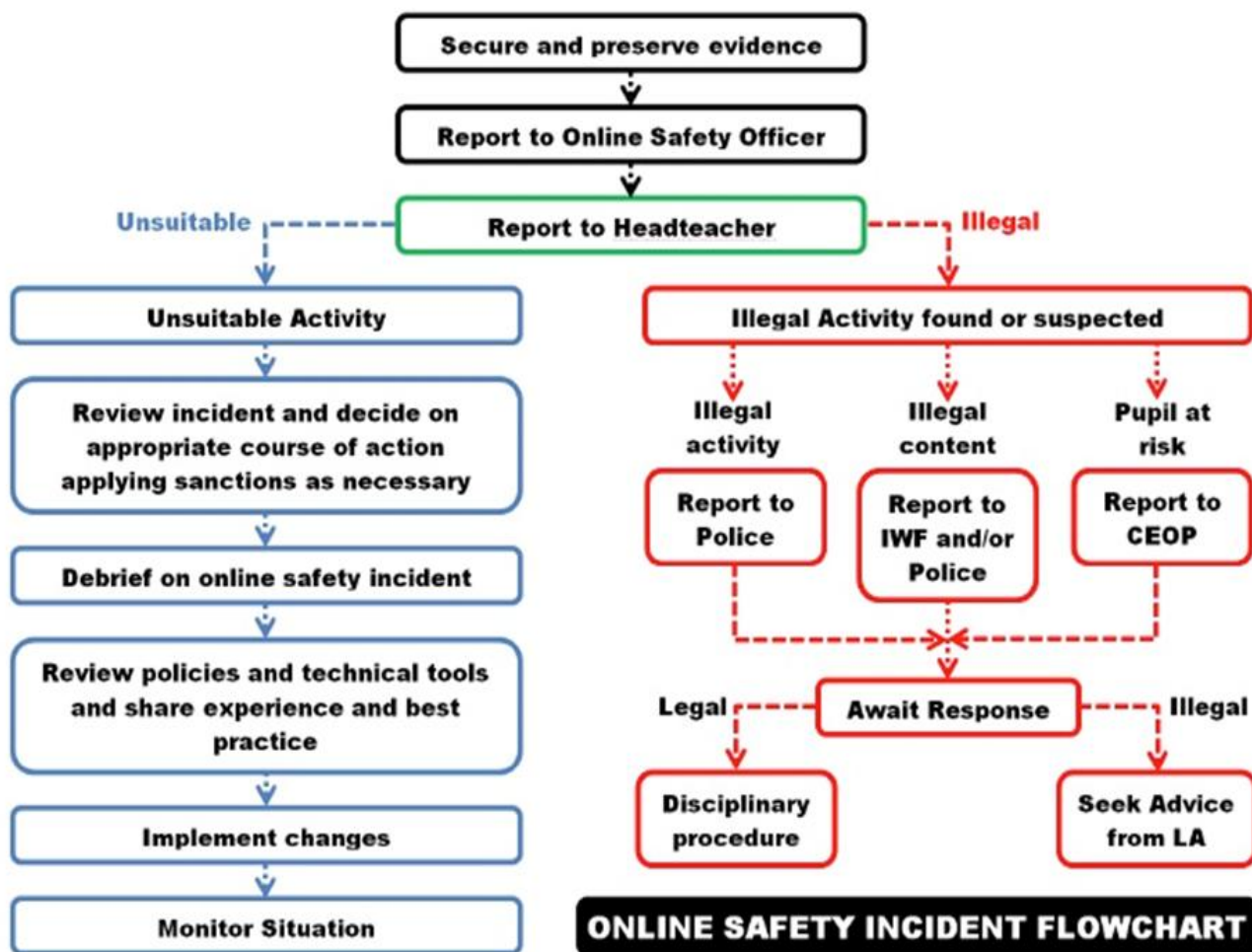
The teacher/responsible adult must:

- 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 learner/learners).
- Report the details of the incident to the DSL/Online Safety Officer.
- If possible, copy and paste the web page address and send it to the DSL/Online Safety Officer.

The DSL/Online Safety Officer will then:

- Log the incident and take any appropriate action.
- Where necessary report the incident to IT Support and RMsafetynet so that additional actions can be taken.

Online Safety Flowchart:



12.3 Online Safety Log

The Online Safety Incident Log and Form is to be completed in collaboration with the DSL and Online Safety Officer (Faye Miller)

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: _____

DSL/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, learners.

Passwords must have a 'strength' of at least 12 where a letter is 1 and a number or punctuation mark is 2. 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:

Run, run as fast as you can – You can't catch me, I'm the Gingerbread Man!

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:

- Names and dates of birth for both staff and pupils.
- Images of staff and pupils that confirm their identity and can be linked to additional personal information.
- National Insurance numbers.
- Addresses of staff and pupils.
- Recruitment information.
- Financial records, such as tax information and bank details.
- Information relating to pupil behaviour and school attendance.
- Medical records, including GP names and medical conditions.
- Exam results and class grades.
- Staff development reviews.
- School assessments and marks.
- Safeguarding information, including data related to SEN assessments.

Non-sensitive data thus includes:

- General teaching plans
- Curriculum materials
- General correspondence of a non-personal nature

12.6 Fair processing notice

Pupil data is essential for the schools' operational use. Whilst most of the pupil information you provide to us is mandatory, some of it requested on a voluntary basis.

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and / or the Department of Education (DfE).

We collect and use pupil information, for the following purposes:

- to support pupil learning
- to monitor and report on pupil attainment progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to keep children safe (food allergies, or emergency contact details)
- to meet the statutory duties placed upon us for DfE data collections

We routinely collect information and may need to share it with:

- schools that the pupils attend after leaving us
- our local authority: Information about attendance at classes. Information about your academic progression and performance.
- The Department for Education (DfE)
- YJST (Youth Justice Support team)
- CAMHS (Child and Adolescent Mental Health Services). This covers general processing to support wellbeing or risk assessment purposes.
- Offsite education providers
- Examination Boards/ Awarding Bodies
- School Nursing Team Berkshire Healthcare NHS Foundation Trust

Work Placement: Where a learner's course involves undertaking a work placement, a project which is delivered by a third party (i.e. where they undertake a period of study at a separate education provider) it will be necessary for their data to be shared between iCollege and the other organisation.

Occupational Health: If a staff member has an additional learning support need, they can access a range of support services through the Additional Learning Support (ALS) team WBC.

Counselling Services: This service provides counselling and other support in respect of wellbeing and mental health.

Youth support services for Pupils aged 13+

Holding data and hosting systems

Much of the personal data will be held in electronic form in systems provided or hosted by West Berkshire Council and iCollege, including systems we have procured from third party providers.

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

12.7: 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 learners, they are asked to sign this code of conduct. Members of staff should consult the iCollege ICT & Online Safety Policy as well as the AI policy for further information and clarification.

- 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, 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 IT support..
- 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 learners, 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 learners (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 learners in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that learners use of the internet is consistent with the school's Online Safety Policy.
- When working with learners, I will closely monitor and scrutinise what they 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 learners' safety to the appropriate person- DDSL/DSL & Online Safety Officer.

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:

12.8 Unsuitable / Inappropriate activities

Unsuitable activity

- Use of personal electronic devices to store school related information
- Posting offensive or insulting comments
- Posting comments that affect professional standing and integrity
- Contacting pupils by email or social networking
- Pupil phone/ tablet/ computer used in school
- Pupils entering personal information online
- Pupils chatting online to others outside school without adult permission
- Viewing material that causes distress (if illegal, then report under illegal activity)
- Taking images/ videos without consent
- Disclosing personal passwords

Illegal Activity found or suspected

- If you've witnessed or been the victim of crime please report it to us www.thamesvalley.police.uk or call 101.

Is someone in immediate danger? Do you need support right away? If so, please call 999 now.

- Hatred on the grounds of your race, religion, sexual orientation, transgender identity or disability.

Report Hate Crimes: <https://www.report-it.org.uk/>

- Report Articles, images, speeches or videos promoting terrorism or encourage violence

https://www.report-it.org.uk/terrorism_and_extremist_material

- Online sexual abuse, online grooming, grooming online

Make a report to one of CEOP's Child Protection Advisors:

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

Sign:		Sign:	
Jacqueline Davies		Tim Pritchard	
Head Teacher		Chair of Governing Body	
Date:		Date:	

Change Record				
Version Number	Date Approved	Management Committee(MC)Minute Reference	Description of Amendments	Review Date
V4	MC 30.11.17	Management Committee	Complete re-write	Sept 2017
V4.1		MC	Update included GDPR and KCSIE updates	Dec 2020
V4.2		MC	Updated links and removed sections that are n/a or used, updated UK GDPR section and definitions of sensitive data	5/12/22
V 4.3	12.12.23	MC	Updated Links, updated KCSIE and CP information, DSL responsibilities 17.11.23 MR + FM	
V5	03.03.26	MC	Admin, formatting and role name changes, links to AI policy-FM	Feb'26

Keeping Children Safe in Education

All staff at iCollege take seriously their responsibility to protect and safeguard the welfare of children and young people in their care; this includes providing help and support to meet the needs of children as soon as problems emerge; protecting children from maltreatment whether that is within or outside the home, including online; 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.

Further info.

The 4 Cs of online safety

An important step in improving online safety at your school is identifying what the potential risks might be.

KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract).¹ These are known as the **4 Cs of online safety**.

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see [illegal, inappropriate or harmful content](#) when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of [grooming](#) or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, [online bullying](#). Conduct also includes things like [sharing or receiving nudes and semi-nude images](#) and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.