Clovelly House School
Stay safe, respect, achieve

E-Safety Policy

January 2026

Content

E-Safety Policy

1. Purpose

The purpose of the policy is:
* to safeguard children from unsuitable internet activity and contacts
* to ensure that all staff and pupils know their responsibilities towards internet safety
* to have a clear policy on acceptable use of the internet by staff including appropriate use for work and personal use and how this will be regulated
* to put structures in place to protect the personal e-space of pupils and staff members
* to ensure that risk assessments are in place to minimise and manage risk with regards to the internet
* to provide clear guidance on the use of images
* to provide clear guidance concerned with copyright and plagiarism.

2. Roles and Responsibilities

The **Head teacher** will ensure that:
* internet safety policies are in place in the school and oversee their implementation
* internet safety policies are linked to other policies in the school such as Child Protection, Health and Safety, Behaviour and Risk Management and Confidentiality Policies
* all role players are familiar with the internet safety policies
* suitable staff members are appointed to take responsibility for co-ordinating all internet safety issues
* all staff members and pupils are fully aware of their responsibilities for internet safety
* all staff members and pupils are aware of their individual responsibilities to protect the security and confidentiality of the school networks by protecting the security of passwords and ensuring that all internet access by pupils is monitored
* the policy is supported by clear procedures should incidents of misuse occur which will result in sanctions such as a disciplinary enquiry, immediate suspension, dismissal and possible police involvement
* pupils are continually reminded about internet safety guidelines
* the policy is regularly reviewed and updated
* the policy is consistent with local and national policies.

Parents and Carers will be:
* consulted on the implementation of the Internet Safety Policy
* made aware of the precautions that the school is taking to ensure a safe ICT learning environment
* made aware of the standards of behaviour and acceptable use that their children are expected to abide by whilst at school
* be involved in drawing up risk assessments to protect individual children
* encouraged to support the school policies through promoting internet safety at home.

The **school** will:
* ensure that there are an acceptable number of computers in satisfactory condition for pupils to maximise learning
* maintain ICT equipment to ensure satisfactory use
* require a standard disclaimer to be attached to all external email correspondence stating that views expressed are not necessarily those of the school or the company
* ensure that anti-virus protection is provided on all staff and pupils computers which is regularly reviewed and updated
* take reasonable measures to monitor the use the internet and email by staff and pupils in accordance with the Data Protection Act 1998.
* have internet filtering systems in place to prevent pupils from accidentally accessing inappropriate materials or use removable dongles for accessing WiFi
* employ technological systems to minimise spam

Education staff members will:
* be issued with Clovelly House School email addresses for work to minimise the risk of staff receiving unsolicited or malicious emails

* check all removable media, (floppy disks, CD-Roms and USB storage devices) for viruses
* report any problems to the ICT teacher and to the Lead Teacher without delay
* not take or store digital images of individual pupils without the written permission of the Head teacher and the child's carers/parents
* be permitted to use their own phones during the school day to access support from the senior staff member 'on call', but they should not use the phone for personal use
* ensure that, if they use a personal mobile for 'on call' purposes, it is secure in order to minimise opportunities for pupils to access it
* report accidental access to in appropriate materials to the line manager and Head teacher immediately
* report any suspected misuse of the internet by colleagues to their line manager and/or the Head teacher immediately

Pupils will:
* be made aware of internet safety policies, including their responsibilities for reporting accidental access to inappropriate materials to education staff members
* be encouraged to contribute to school internet safety policies
* be made aware of the sanctions for accessing inappropriate materials leading to internet sanctions or, in serious cases, police involvement
* check all removable media, (floppy disks, CD-ROMs and USB storage devices) for viruses and report any problems to the ICT teacher and to the Head Teacher without delay
* not use school equipment to access personal emails or personal accounts during school time
* use their personal logins for their own use and ensure that the teacher is aware of the password

3. E-Safety Training

Education staff members
* All education staff members will undergo relevant e-safety training for the particular role they hold in the school including information on Clovelly House School's acceptable use policy
* All staff members will receive training on how to search for and evaluate information safely on the internet
* All staff members are required to update their knowledge about the risk assessments concerned with internet use for individual pupils
* All staff members will have training on the reporting and recording procedures concerned with breach of internet protocols
* Staff members will be trained to incorporate internet safety activities and awareness within their curriculum areas and to monitor, support and co-ordinate these across the school

Pupils
* Pupils will have lessons in internet safety and awareness across the curriculum
* Pupils will be constantly reminded about internet safety including updated information involving new and emerging technologies
* Pupils will be taught how to critically evaluate materials as well as learning good searching skills
* Pupils will be taught appropriate strategies for dealing with spam
* Pupils will be made aware of relevant legislation when using the internet relating to data protection and intellectual property which serves to protect them and to develop academic integrity
* Pupils will be taught to differentiate between materials which they may legally download such as copy-right free resources and those prohibited such as games and music
* Pupils will be taught about the impact of internet bullying from the perspective of both the bully and the tormentor and will be encouraged to seek help from staff members, or organisations such as 'Childline' if this occurs

Chat rooms
* Pupils will not be permitted to use social media platforms at school
* Pupils will be taught about the importance of safely negotiating online relationships
* Pupils will be made aware of the importance of keeping personal information private when chatting
* Pupils will be made aware of the dangers of arranging offline meetings with people they have met online

Instant messaging

* Pupils will not be permitted to use instant messaging services within school
* Pupils will be taught about safety issues relating to instant messaging
* Pupils will be taught how to protect personal information when registering for instant messaging services and how to set up closed groups or buddy lists
* Pupils will be made aware of where to get help and advice if they experience problems such as unwanted messages or bullying by instant messaging

Mobile phones and other portable devices
* Pupils will not be permitted to use mobile phones and other portable devices at school other than for education or for self-regulating purposes outside of lessons
* Pupils will be taught about safety issues relating to mobile phones and other portable communications devices such as personal digital assistants, (PDAs)
* Pupils will be made aware of the risks of always being accessible, (and hence possibly excluded from other forms of social contact), the possibility of receiving inappropriate and unsolicited contact by text messaging, text overuse and misuse and bullying by mobile phone
* Pupils will be made aware of new forms of service and content which are increasingly available via mobile phones, such as picture and video messaging, Bluetooth, commercial content and location-aware services and the safety issues relating to these
* Pupils will be made aware of how to protect themselves from mobile phone theft and of the procedures for reporting the IMEI (International Mobile Equipment Identity) number, hence disabling the phone if it is lost or stolen

Camera phones
* Pupils are not permitted to use personal camera phones at school fro the purpose of taking photographs
* Pupils will be taught abut safety issues relating to camera phones such as having their photograph taken without their knowledge or permission or taking photographs of others without their permission or knowledge

Peer to peer networks
* Pupils will not be permitted to access online peer to peer networks within school unless it is part of a specific managed lesson
* Pupils will be made aware of safety issues relating to peer-to-peer networks
* Pupils will be made aware of the risks of viruses and of the need to virus check any materials downloaded and install firewalls on their own machines
* Pupils will be made aware of their responsibilities of illegally downloading or uploading materials to peer to peer networks

e-Portfolios
* Pupils will have personal passwords and will store their own work on their own account
* Staff members will be able to view pupils' work at any time
* Other pupils may view pupil work only if agreed by the owner of the content and by a supervising staff member
* Pupils may not upload, download or store any material which is deemed to be inappropriate by any staff member
* Pupils will always be supervised by staff members whilst using the computer and the staff members will verify the validity of the information contained within e-Portfolios
* Staff members will monitor and ensure that material for coursework is stored safely

Webcams
* If webcams are used within school for curriculum activities such as video conferencing the Head teacher must be informed
* If webcams are used within school detailed and appropriate risk assessments must be in place to manage risk connected to use of webcams
* If pupils have access to webcams at school, they must be fully supervised by staff members
* Pupils will be made aware of safety issues concerned with using webcams outside school such as inappropriate contact and Trojan horses which might activate a webcam without their knowledge

4. Acceptable use of ICT facilities within the school

* Subject teachers will be encouraged to use ICT across the curriculum
* Subject teachers will organise the environment to ensure that pupils have safe access to suitable computer facilities
* All pupils will have access to ICT lessons in addition to cross curricular ICT work
* Access to the internet will be determined for each pupil and for each site in consultation with the Head teacher and with risk assessments in place
* If pupils have direct internet access, this will be secured through a remote access which may be turned off by staff members at any time if necessary
* If pupils have internet access through dongles, these will be kept securely be staff members and will be locked away when not in use
* If pupils use their own laptops, these will be subject to the same policies and procedures as school equipment
* If the school laptop is used, pupils will be monitored at all times
* If portable devices, such as memory sticks and CDs are used, these must not contain any personal information and their use for school must be supervised by a staff member
* If staff members use their own laptops for school these must be secured with a password and any use by pupils must be supervised using a guest password
* All ICT equipment must be PAT tested to ensure that it has passed an electrical safety test
* If pupils use computers outside of lessons, they must be supervised by staff members
* Members of the community and visitors will not be permitted to have access to the school computers without permission from the head teacher and the Assistant director

5. School website

* The school website must be approved by the Director and senior managers of Clovelly House School
* Only content that is uploaded by the Administrators and the Head of ICT will be allowed on the website
* The website will be checked regularly by the Head teacher and the Head of ICT to ensure that there is no content that will compromise the safety of pupils or staff
* The website will not contain images or any details of pupils
* The school website will not use facilities such as guest-books, notice-boards or weblogs
* The school website will not infringe on intellectual property or the rights of others through any of the materials available on the website
* The material on the school website is the property of Clovelly House School and may not be copied for any reason other than to inform stakeholders of information about the schools such as the school brochure, policies and procedures, OFSTED reports and information about external examination results
* Anyone who accesses the school website will be required to register their interest electronically

6. Filtering and monitoring systems

According to the Government Guidance, 'Keeping Children Safe in Education, 2023', the school will ensure that filtering and monitoring systems are regularly updated and monitored to limit children's exposure to unsuitable materials on the internet. All staff will be aware of this and the DSL will oversee the management of filtering and monitoring systems.
Additionally, all parents will be informed about what systems the school has in place to filter and monitor online use, what staff are asking children to do online, and, who, from the school their child will be interacting with online.

7. Consequences for misuse of ICT in the school

Staff members

* If staff members are found to have breached e-safety procedures in or out of school the Head teacher should be informed immediately. If the breach involves the Head teacher then the Senior Leadership Team must be informed immediately
* If there are children protection concerns, the company child protection officer must be informed

immediately
* The Head teacher and/or the assistant director and/or the child protection officer will make a decision whether to refer the matter to the police for investigation and the staff members may be suspended pending a police investigation
* If the decision is made not to involve the police initially, staff members who breach e-safety procedures at school will be subject to a disciplinary enquiry
* The outcome of a disciplinary enquiry may result in a formal warning, dismissal and/or legal proceedings if necessary

Pupils

* If a pupil brings mobile phones or portable devices into school s/he will be asked to hand them in to the staff member and they will be kept locked in the office until the end of the day when they will be handed back to care staff
* Pupils who need their phone for self-regulation, may be permitted to hold on to their phone, providing it is not used during lessons
* If a pupil is breaching the rules and they refuse to hand in the phone or portable device, where possible, the home will be informed and they may be sent home. If they then leave the phone at home they should return to school
* If pupils misuse the internet at school, they will have a sanction on the use of the equipment and risk assessments will be in place for further use of the equipment
* If pupils are found to have breached e-safety procedures in or out of school the Head teacher should be informed immediately and the School Head will make a decision about whether to inform the Bursar and Principal
* If there are child protection concerns, the company child protection officer must be informed immediately
* The School Head and/or the DSL will make a decision whether to refer the matter to the police for investigation and will put procedures in place to work with the pupil pending a police investigation

8. Policy Monitoring

* All stakeholders will be consulted and involved with establishing this policy
* This policy will be monitored and reviewed annually, or more frequently if additional risk management is Required

9. Artificial Intelligence

Our school promotes the use of AI to benefit the curriculum in place. The AI used for curriculum purposes must be formally recorded via a Data Protection Impact Assessment and stored in the Data Protection folder. All AI generated lessons, planning, schemes of work or resources must be thoroughly checked and monitored for errors by staff members before being implemented. We ensure that all students are supervised on devices that can access elements of AI to ensure overall safety from information gained or potential misuse of such platforms. Please refer to Generative Artificial Intelligence Policy for further information.

See also: Clovelly House School Policies and Procedures on ‘Internet Usage’
Leicestershire CYPS E-safety Policy
Clovelly House School ‘Positive Behaviour Management Policy’
Clovelly House School Risk Assessments
Safer Children in a Digital World, Byron Review
Curriculum Policy
Teaching and Learning Policy
Assessment Policy
SEN Policy
Marking Policy
Homework Policy

Appendix 1

Notes on securing and preserving evidence

School premises
Following any incident that may indicate that evidence of indecent images or offences concerning child protection may be contained on school or home computers, the matter will be referred at the earliest opportunity to the local safeguarding board.
The school will not commence its own investigation prior to involving the police for the purpose of preserving valuable evidence both on and off the premises where suspects may have inadvertently become aware of raise suspicions.
If a computer is suspected to contain illegal material it will not be used or viewed by anyone except the investigating police officer.

Home computers
If a student discloses potential crimes involving computer-based media the police may be involved to obtain a forensic copy of the pupil's home computer to preserve any evidence. This will be conducted discreetly, and the computer will be returned when the process is completed. However, there will be legal consequences if illegal material is discovered on the computer.

Appendix 2

Clovelly House School Procedures for Acceptable Internet and e-Mail Use

This policy covers the use of the Internet and e-mail systems for both business and private use. It is designed to protect the interests and needs of both the company and the employees in determining how these systems can be used.
This policy is designed to raise awareness of the potential personal and commercial risks of using these systems and to ensure that all employees understand their responsibilities and the company expectations in the manner in which these systems are used. In setting and monitoring these standards, the company will comply with the individual rights of employees and any further legislative requirements.
This policy applies to all employees, consultants and other workers within the company, whether full or part-time, as well as agency workers, temporary workers and contractors.
This policy does not form part of your terms and conditions of employment and may be amended from time to time. However, all staff members are requested to sign a written declaration stating that they have read and understood this policy.

USING THE SYSTEMS
As part of your job you may be required to use the company internal and external e-mail systems and the Internet.
The company reserves the right to monitor, retrieve and review all e-mails you send, receive or are composing on an ongoing basis or as part of any specific investigation. The company also reserves the right to monitor your use of the Internet, including downloading files in any format on an ongoing basis or as part of any specific investigation. Such monitoring is for the purposes of car, security and compliance with this policy.

You must not intentionally or recklessly upload, down-load or distribute any materials that are or may be interpreted to be defamatory, abusive or offensive to any other individual or organisation. A claim of defamation or discrimination may be brought against you and/or the company if you do not comply with these provisions.

Access the company e-mail server is protected by a firewall which prevents unauthorised external access via the Internet. Never accept or open any file as an e-mail attachment if you are in any doubt about the source.

Using e-mail
E-mail can be an effective form of communication, but care must be taken to retain an appropriate level of formality when dealing with colleagues and other individuals with whom you may come into contact during the course of your employment. You must take care to protect the reputation of the organisation at all times.
E-mails should be checked each day that you attend work.
You should obtain confirmation of receipt for important emails sent.
You should make and keep hard copies of important emails.
Emails can form legally enforceable contracts that should bind the organisation. These should only be entered into with proper authorisation. Care should be taken when expressing your personal opinion as this could be construed as the opinion of the organisation. All e-mails must contain the organisational standard disclaimer.
All e-mails, whether in hard copy or held on the computer system, are potentially disclosable documents for the purposes of litigation, and therefore should be treated with care accordingly. However you should be aware that deletion of a message or file will not fully eliminate it from the computer system.
E-mail communication is inherently in-secure and you must therefore avoid sending confidential or secure information via email. The same obligations to keep information confidential apply to information contained within an email as to other forms of communication. Other members of the organisation or the public may have access to email messages and accordingly confidential information should never be sent via email or the Internet including to your home email address, unless you have the express written permission of the Head following consultation with the Operations manager. You are required to use initials of people you are referring to in order to protect the integrity and authenticity of messages sent.

You should regularly delete old messages to avoid filling up storage space.

DOWNLOADING AND INSTALLING SOFTWARE

You must not download or install any computer programmes or other software on the computer system that has not first been authorised by the office manager. This includes games, screensavers, animations and other graphics files. This is to prevent the downloading of viruses into the organisational computer system.
All computer programs and materials on the internet are protected by copyright and you should take care not to infringe this by, for example, making copies of programs, graphics or text.
The organisation has a number of software licenses to use the applications installed on your computer and you must not download or install any unlicensed programs.
You should also take care when using information that you have downloaded from the internet as unauthorised use by you could infringe the copyright of original owner.

COMPUTER EQUIPMENT

Should any operational problems arise with your computer equipment, you should report this to the Office manager immediately. Only personnel agreed by the ICT manager can dismantle, repair or upgrade your computer equipment. You must not attempt to do any of these things on your own account.

PASSWORDS AND ACCESS

You should never attempt to access another individual's computer, nor should you attempt to gain access to information beyond the level to which you have been assigned access.
All passwords should be recorded and kept in the safe at the admin centre.

PROHIBITED ACTS

The following acts are strictly prohibited:
* sending confidential email to or from an address which is not secure (e.g. home computer, not an organisational address, LA, etc.) If you are unsure whether an email address is secure, ask for guidance for the ICT manager. Do not send information to a home email address without the prior written authorisation of the Head following consultation with the ICT manager, even if you believe that you home email address is secure.
* on-line gambling
* accessing, downloading, displaying or distributing pornography
* accessing, downloading, displaying or distributing information that may cause harassment to others on any grounds
* participating in chain letters
* making defamatory, false of misleading statements
* creating a hyperlink between the organisational website and any other website
* providing your email address on a website
* subscribing to websites or downloading information where payment of a fee is required, without authorisation
* altering the search engine to anything other than a recognised site e.g. Microsoft, Google, etc.
* Installing Hot Bar on the computer
* accepting or opening any file received as an email attachment if the source in in doubt in an way

PERSONAL USE

A certain amount of personal use of the email and Internet system is permitted by the organisation, provided that this does not interfere with your normal activities. Privacy cannot be guaranteed and you may therefore wish to consider alternative methods of communication as appropriate.
You are reminded that all the provisions of this policy will apply to such personal use.

LAPTOPS AND PORTABLE COMPUTING EQUIPMENT

The use of laptops and portable computing equipment that are provided by the organisation are covered by all the provisions of this policy, whether on company premises or not.
Particular care must be taken over the security of the equipment, the software and data stored on it.
You are not permitted to use a laptop not owned by the organisation on any organisational premises without the express written permission of the Head following consultation with the ICT manager.

DATA PROTECTION

You should comply with the requirements of the data protection act 1998 in terms of obtaining using and communicating personal data held electronically about any individuals.

BREACH OF POLICY

If you are found to have breached this policy in any way, the organisational disciplinary procedure will be invokes against you and you may be subject to disciplinary action, up to and including dismissal with or without notice. Such disciplinary action will be invoked particularly in respect of excessive use of the Internet or email facilities, failure to ensure the security and/or confidentiality of information sent or received by electronic means and the downloading, displaying and distribution of pornography or other materials causing harassment and distress to other individuals.

You should also be aware that the downloading and distribution of pornography can constitute a criminal offence. If, in the course of a disciplinary investigation it is found the you have committed such an offence, the organisation reserves the right to report such behaviour to the police.

If you believe that the organisation has breached this policy in any way you should raise a grievance under the organisational grievance procedure.

If you believe that you have been subjected to behaviour which is discriminatory or harassing as a result of another employees use of the systems you should make a complaint under the organisational Equal Opportunities Policy.

Appendix 3

Use of Internet Contract for Pupils

1. I shall behave responsibly when using the internet.

2. I will not go onto sites which are not allowed.

3. I will be sensible whilst using the Internet.

4. I will use the internet for school-work and research.

5. I will follow the instructions given by the teacher at all times.

6. I will report any unsafe materials that I find on the internet to the teacher.

7. I will not copy material that I find on the internet without checking with the teacher that I can use it for school-work.

8. I will treat the equipment with respect.

9. I understand that if I use the Internet in an inappropriate manner, my right to use the internet will be taken away.

Signed:

Pupil: …… Date: ……

Teacher: …… Date: ……

Appendix 4
Flowchart for responding to internet safety incidents in school