Internet Safety Policy

2024-2025

Learning to Flourish

To provide Personalised learning experiences so that every child can communicate, interact, grow and develop to the best of their ability. Together with families, we can ensure that our children have the skills and knowledge to manage everyday life as independently as they can and to lead happy and successful lives, through our values of **S**ocialisation, **C**ommunication, **I**nteraction, and **P**lay

Introduction

At The Hollies School, we strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

- Access to worldwide resources and research materials
- Educational and cultural exchanges between pupils worldwide (Skype for instance)
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA, WG and D of E)

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web-based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy. The Aims of this Acceptable Use Policy are to:-

- Allow all users access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.

- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.

- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

Writing and reviewing the online safety policy

The school has a designated online safety coordinator.
The online safety policy has been agreed by the senior management team and approved by the governors. It will be reviewed on an annual basis.

Acceptable Use Policy

At The Hollies School, we acknowledge the educational and social benefits of ICT facilities. All staff (including supply staff and temporary staff) and pupils must adopt a common-sense approach to the use of ICT equipment and software that gives due consideration to social and legal obligations. Inconsiderate or inappropriate use of facilities may result in disciplinary action, exclusion and possibly even legal action.

ICT facilities should normally only be used in connection with work associated with the school and not for personal or private communication. Limited and appropriate personal use is acceptable, for example during the lunch breaks or before or after the school day. Computer facilities must not be used to offend or harass, either within or outside the school. Individuals should never disrupt, interfere with or prevent anyone else using the facilities legitimately. Certain acts are considered particularly inappropriate and will lead to action under the relevant staff or young person Disciplinary Code and Procedures.

In the case of staff, the following acts may be considered to constitute gross misconduct and could lead to dismissal:

- the use of computer facilities to offend or harass;

- the sending or relaying of sexist/racist/defamatory/indecent /obscene/ pornographic/ violent/offensive e-mails, data or images;

- the accessing of sexist/racist/indecent/defamatory/obscene/pornographic/ violent/offensive material;

- the downloading, storage and distribution of such material including the creation of a website or screen saver of such material;

- the use of the ICT facilities for commercial gain or for work on behalf of others unless prior agreement has been made with the designated authority;

- the deliberate misuse of the network or networked resources, such as introducing “viruses”, violating the privacy of others;

- the theft, abuse or willful damage of computer equipment;

- the misappropriation of software belonging to another person or institution; and

- the sale, import and distribution of copies of software without the permission of the copyright owner.

The above list is not intended to be exhaustive, but an indication of the types of act that would be dealt with under the Disciplinary Code and Procedures.

In addition to the list above, staff are discouraged from being members of social networking sites. However, if staff are members they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

General Internet use and Consent

Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.

Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. (Appendix 1) The school will keep a record which will be regularly referred to by teachers and monitored by the Headteacher and admin staff. The use of the names of pupils or photographs of pupils for websites will require written permission from parent(s)/guardian(s) included on the consent form. If a picture is placed on the website the child’s full name will not be displayed.

Pupils must not use the school ICT facilities without the supervision of a member of staff.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the assistant head and the esafety lead immediately who will, in turn, record the address and report on to the Head Teacher and Internet Service Provider.

Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)

Staff and Governors must agree to and sign the Acceptable Use Agreement (appendix) each year.

Monitoring of Systems

The Hollies School gives notice of its ability to monitor and intercept information for the purposes of:

- Establishing the existence of facts (e.g. to obtain evidence of business transactions);
- Ascertaining compliance with regulatory or self-regulatory practices or procedures;
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using its systems (e.g. for staff training or quality control);
- Preventing or detecting crime
- Investigating or detecting unauthorized use of the system (e.g. to check that users are not downloading pornography);
- Ensuring the effective operation of this system (e.g. to protect against “viruses”, “worms”, denial of service attacks, unauthorized access).

Monitoring is allowed under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000, but is also subject to the provisions of the Human Rights Act 1998 and the Data Protection Act 1998.

Authorised IT Systems Administrators require access to data held on ICT equipment or transferred over the network to ensure that networks, systems and services are operating correctly. Any information obtained in the course of such duties will be treated as confidential unless it is thought to indicate an operational problem.
Any information obtained in the course of these duties that is thought to indicate misconduct or breach of school policies will be brought to the attention of the Head Teacher. If deemed appropriate, further monitoring of IT and network equipment may be carried out to ensure compliance with school policies which apply to these systems. Monitoring of an individual’s ICT facilities will only be carried out when there is reason to suspect misuse and will only be carried out at the request or authorisation of the Head Teacher.

Log in and Passwords

Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.

Pupils and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.

Staff and pupils must ensure terminals, laptops or any ICT equipment (iPads etc.) are logged off (or hibernated) when left unattended.

Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user. Protect your work area; do not tell anyone your password. The password is displayed on screen as a line of ******, however people watch fingers and it is quite easy over a period of time to work out what the password is, so be careful. Anyone who needs assistance in changing his or her password should contact the Schools ICT Service.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.
Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities.
Some forms of cyber bullying are different from other forms:

Through various media, children can be cyber bullied 24 hours a day.
People who cyber bully may attempt to remain anonymous.
Anyone, of any age, can cyber bully.
Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention

We recognize that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided.

We recognize we have a shared responsibility to prevent incidents of cyber bullying but the Head Teacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber Bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has.
ICT safety is integral to teaching and learning practice in the school.
Parents are also made aware of cyber bullying and their responsibilities for supporting safe ICT use (see Appendix 1).

Record Keeping and Monitoring Safe Practice

As with other forms of bullying, the Head Teacher keeps records of cyber bullying. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying. However, we monitor internet use on a regular basis as a disincentive for bullies misusing school equipment and systems. The ICT Coordinator will conduct regular use checks, log any concerns and inform the Head Teacher.

Online safety

Children and staff are reminded of Online safety Codes of Conduct at the start of each academic year. Online safety posters are visible in every class or work area involving ICT.

Any work or activity on the Internet must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden.

Staff are discouraged from being members of social networking sites. However, if staff are members, they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

Do not give personal email or postal addresses, telephone / fax numbers of any person.

Under no circumstances give email or postal addresses / telephone numbers / fax numbers of any teachers or pupils at school.

Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and increase the workload of the IT staff.

Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.

Users should assume that ALL software is subject to copyright restrictions, including shareware. Pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of the ICT Co-coordinator before attempting to download or upload software.

All software, including applications for iPads or other mobile forms of ICT must be purchased via the ICT Coordinator or Head Teacher. Unauthorised or non- standard software may not be installed unless prior consent from the ICT Coordinator is obtained.

Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or ICT coordinator.

If in doubt, DO NOT USE.

The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

School Network and Pupil Files

Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area.

Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.

The ICT Coordinator and SLT can view any material pupils store on the school's computers, or on memory sticks/disks pupils use on the school's computers.

Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask the Head Teacher or ICT Coordinator for advice.

Users accessing software or any services available through school facilities must comply with license agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

Security Guidelines

Backups

Files stored on the network are backed up regularly. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore. Back-ups are kept securely at county hall

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable, but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. (See above)

Use your Network Area

Always ensure that files are saved to your network area (class folders on the Teacher Shared area of the network), or your school OneDrive folder on Teams, NOT only on the local hard drive. This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Off-site pupil data and pupil information

Lap tops, iPads and back-ups (USB sticks) may be taken off site. Staff are to ensure that lap tops and iPads are used cautiously when viewing pupil data/information and images and that lap tops are logged off when left unattended. Staff are encouraged to use OneDrive/Teams to back up and store files when off site. Images must be transferred to the school network as soon as possible to be removed from the mobile device. Data, images and pupil information must be removed from OneDrve/Teams and laptops when pupils transfer to another class to avoid records being kept of pupils that are not taught by their former teacher.

Virus Checks

All computers in school have anti-virus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT Coordinator straight away.

E-Mail Usage

Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer

When using e-mail, pupils and staff should:

- Not access personal emails in school using school equipment.
- Be aware that e-mail is not a secure form of communication and therefore pupils should not send ANY personal information.
- Should not attach large files
- Must not forward e-mail messages onto others unless the sender's permission is first obtained.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Must not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated

This Guidance will apply to any inter-computer transaction, be it through web services, chat room, bulletin and news group or peer to peer sharing.

Mobile Devices

Any mobile device provided to staff by The Hollies School, including iPads, remain the property of the School. These devices are for school use only. These devices will regularly need syncing/updating and will need to be returned to school for this purpose. Any personal information that is deemed inappropriate will be removed and that device will not be returned to the member of staff. In these circumstances, it would be dealt with under the Disciplinary Code and Procedures.

Pupils are not permitted to bring mobile phones or devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the School Office to look after during the school day and collected at the end of the day.

Pupils may not make personal calls from a mobile phone during the school day.

Mobile phones may not be used to take pictures of pupils and staff (use devices provided by the school)

Pupils should not send or receive email or text messages to/from their mobile device during the school day.

Any inappropriate use of mobile devices such as cyber bullying must be reported to the Head Teacher (see Cyberbullying)

Staff should only use their mobile phones at appropriate times of the day only e.g. break-times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

Any pupil who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day (in accordance with the school's Behaviour Policy). The device will be secured in the school safe.

Social Media

The Hollies school has a dedicated website for communicating with parents, as well as a social media Twitter account. These are only to be used by authorised persons and will only be used for information purposes only. Photo permission will be sought before pictures of staff and pupils can be used. It is the responsibility of the class teacher to ensure that pupils have permission before appearing online.

GDPR

As outlined in the school policy for Data Protection (GDPR) and the policy for Information Security, we never assume consent for using pupil images online or transferring pupil information electronically. Anything outside the scope of the school privacy notice will require additional consent from parents. Parents have the right to withdraw consent. This may lead pupils having limited access to ICT systems in school. For more information about parents' rights, refer to the schools Data policy.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the ICT Coordinator or Head Teacher to discuss the situation. Solutions are possible! Remember also that shareware is not freeware and must be licensed for continued use.

Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Head Teacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's

copyright. “Acquisition” includes loading a copy of a programme into the random-access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at anytime. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

“Hacking” is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

If pupils break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Video-Conferencing and Webcams

The use of webcams to video-conference will be via a filtered service. Publicly accessible webcams are not used in our school setting.
Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Managing Allegations against Adults Who Work With Children and Young People

Allegations made against a member of staff should be reported to the Senior Designated Person (SDP) - Ms Lisa Marshall - Head Teacher, for safeguarding within the school immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Additional Information

Please be aware, at such time that you leave The Hollies School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.

If pupils, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Head Teacher for further guidance.

A copy of this policy is available on the school website www.holliesschool.co.uk

The Hollies School

Parent/Pupil Acceptable Use of ICT Agreement/e Safety Rules

• I will only use ICT in school for school purposes.

• I will not tell other people my ICT passwords.

• I will only open/delete my own files.

• I will not bring software, CDs or ICT equipment into school without permission.

• I will only use the Internet after being given permission from a teacher.

• I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

• I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.

• I will not give out my own details such as my name, phone number or home address.

• I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me.

• I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

• I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

The Hollies School
Learning to Flourish

THE HOLLIES SCHOOL
Bryn Heulog, Pentwyn, Cardiff CF23 7XG
Tel: 029 20734411 Email: theholliessp@cardiff.gov.uk
Headteacher: Lisa Marshall

The Hollies School
Pentwyn Drive,
Pentwyn
Cardiff
CF23 7XG

Dear Parents/Carers,

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any ICT.

Please read and discuss with your child the Online Safety rules overleaf and return this sheet signed. If you have any concerns or would like any further explanation, please contact your child's class teacher.

This Acceptable Use of ICT Agreement is a summary of our Online Safety Policy which is available in full, on request or can be viewed on our school website.

By signing this, you are giving permission for your child to use ICT equipment in school. Without this permission, unfortunately we may have to limit the access your child has to ICT equipment.

Yours sincerely,

Mr Chris Cummings
Assistant Headteacher

The Hollies School
Learning to Flourish

THE HOLLIES SCHOOL
Bryn Heulog, Pentwyn, Cardiff CF23 7XG
Tel: 029 20734411 Email: theholliessp@cardiff.gov.uk
Headteacher: Lisa Marshall

Parent's/Carer's Consent for Internet Access

I have read and understood the school rules for Acceptable Use of ICT and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that

the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that should my son/daughter may need to access to the internet outside school, I will take all reasonable precautions to ensure he/she cannot access inappropriate materials and that he/she will use the computer in an appropriate manner.

Signed..... (parent/carer) Date.....

Name of Pupil(s) ……

Acceptable Use Agreement for Staff and Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement:

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting, **including using a personal device during lesson and play times.**
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will 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 or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices
- **I understand that I must follow the EWC code of conduct and guidance for social media. Any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality, whether by email or social media sites, will be classed as a disciplinary matter.**

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name _____ Signed _____

Date _____