Hollywater
SCHOOL
PATHWAYS TO A WIDER WORLD

Hollywater School E-Safety Policy

Approved by Chair of Governors, Silas Jones		**Date:** October 2022
Headteacher: Chris Toner		
Last reviewed on:	October 2022	
Next review due by: (Annually)	October 2023	

Whilst IT is both extremely exciting and highly beneficial to all pupils at Hollywater School, it is important that all users are made aware of the range of risks associated with the use of Internet technologies. At Hollywater we understand the responsibility to educate our pupils on E-safety issues ; teaching them the appropriate skills, knowledge and understanding to enable them to remain safe when using the Internet and other related technologies, in and beyond the context of the classroom. This policy, supported by the **Acceptable Use Agreements for staff and pupils** and the **Safeguarding policy**, sets out how we educate pupils of the potential risks ensuring that we protect the interests and safety of the whole school community.

- **Roles and responsibilities**

There are clear lines of responsibility for E-safety within school. For pupils the first point of contact should be a teacher, a member of staff or Senior Management Team.

All staff are responsible for ensuring the safety of pupils and should report any concerns immediately to the Deputy Head or Headteacher and then record the incident on CPOMS (online safeguarding system). When informed about an E-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

The IT / Computing Co-Ordinator, Sarah Kitching, is responsible for the day to day issues relating to E-Safety. They are responsible for :

- day to day issues relating to E-Safety and take a leading role in establishing and reviewing school E-Safety policies
- ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident
- providing training and advice to staff
- liaising with the Local Authority for guidance and support
- liaising with the school IT technician
- organising and blocking specific Internet sites within the school's filtering system

The Headteacher is responsible for ensuring the safety of all members of the school community alongside the IT / Computing Co-Ordinator. Procedures are in place for the Headteacher to follow in the event of a serious E-safety allegation or incident.

Our Governors are responsible for the approval of this policy and for reviewing its effectiveness.

- **E-safety curriculum**

E-safety is an essential part of the IT / Computing curriculum across all key stages. All pupils need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. This is particularly important for helping pupils to stay safe out of school where technical support and filtering may not be available to them.

An online safety risk assessment, 360 safe review, is carried out annually to enable us to review our online safety policies and practice.

E-Safety education is delivered in the following way :

- A planned E-Safety programme which is part of the Computing and RSHE curriculum throughout the year – this covers both the use of IT and new technologies in school and outside school

- Through the use of a wide range of resources, including the CEOP's Think U Know site as well as resources produced in conjunction with Hampshire Police

- Learning opportunities for E-Safety are built into the school curriculum for Computing / IT

- Key E-Safety messages are reinforced through further input and informal discussions when the opportunity arises

- Pupils are encouraged to adopt a safe and responsible use of IT both within and outside school – Acceptable Use Policy for pupils shared and displayed in IT suite

- In lessons where Internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches

- Signposting information for parents on school website to Government links, information updates and parent guides. Additional support is provided to families as issues or concerns arise.

- E-safety sessions are provided to specific cohorts throughout the year. This includes KS4 session on social media and online abuse and KS2 sessions on keeping safe online as part of the NSPCC programme.

- DSLs complete E-safety safeguarding training and all staff complete annual E-safety training

- **System security**

Hollywater Schools IT system security is constantly reviewed. The virus protection is kept up to date and we continue to work with HCC and Agile to ensure that the system that protects our pupils is reviewed and improved regularly.

At Hollywater we will take all precautions to prevent access to inappropriate 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 computer connected to the school network. Neither Hollywater, HCC or Agile can accept liability for any material accessed. If staff or pupils come across unsuitable on-line materials, the site must be reported to the IT / Computing Co-Ordinator or IT Technician immediately and the necessary action will be taken through HCC and Agile.

All users are provided with an individual network login and password which is unique to them and must not be shared or used by others.

All staff are aware of their responsibility when accessing school data – see **Acceptable Use agreement for staff** for more information. All staff have read the Data Protection policy, carried out annual GDPR training and have read Privacy notices that shares the purpose of why and with whom we are able to share data with.

- **Internet**

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, as well as a potential risk to young people and vulnerable people. Pupils at Hollywater are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.

Hantsnet is a filtered system.

At Hollywater we ensure that all pupils have supervised access to the Internet. See **Acceptable Use agreements for both staff and pupils** for more information.

If members of the community wish to use the Internet at Hollywater then they will also be asked to read the **Acceptable Use agreement** within school. We will maintain a current record of all staff and pupils who are granted access to school IT systems.

- **E-Mail**

Staff and pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive an offensive e-mail. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone.

  - Staff use only the school email services to communicate with others when in school, or on school systems through remote working
  - Users need to be aware that email communications may be monitored
  - A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
  - Users must immediately report, to the IT / Computing Co-Ordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email

- **Use of digital and video images**

Written permission from parents or carers, in regards to photographs, will be obtained at the beginning of each academic year. Verbal permission will also be obtained for use of photographs outside of school e.g. newspaper etc.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

- **Use of web-based tools – publication and assessment**

Our school uses the public facing website, www.hollywaterschool.org.uk, for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of pupils. All users are required to consider good practice when publishing content. Personal information should not be posted on the school website and only official email addresses used.

Only pupil's first names are used on the website, and only then when necessary.

Detailed calendars are not published on the school website.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:

> Pupils' full names will not be used anywhere on a website, and never in association with photographs. Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

At Hollywater School we also use the secure web-based assessment tool Evidence for Learning which enables us to record and share evidence, through photos and videos, with parents regarding pupil progress. The company have shared their Data Protection policy and GDPR compliance statement that ensures that data is only stored in the cloud within the UK. Parent permission to use photos and videos of pupils within the assessment tool is gathered on an annual basis.

As part of this software and also as part of developing parent communication we also use the Parent Portal and Activity Channel. Both of which are secure with individualised links and passwords that enable them to only access information about their child.

- **Social Media**

All staff and pupils are unable to access social networking sites as they are blocked by Hollywater.

Staff and Governors should :

- Ensure that their profile / posts are kept private to friends where possible, this also includes personal information
- Not accept current or ex-pupils as ' friends ' on any social media sites
- Ensure that their communication maintains their professionalism at all times
- Not use these media to discuss confidential information or to discuss specific pupils

Pupils should not be signed up to most social networking sites due to the over 13 age limit. All pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. As a school, we do reserve the right to contact sites and ask them to remove our pupil's accounts should any issues, such as cyber-bullying occur.

- **Use of hand held technology (personal phones and hand held devices)**

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. Personal hand held devices will only be used in lesson time in an emergency or extreme circumstances.

Members of staff are free to use these devices in school, outside teaching time and not in front of children.

Staff and volunteers will not carry personal mobile phones while working. This protects them from being distracted from their work and from allegations of inappropriate use. Phones must be safely stored out of sight of children and should be on silent so that they cannot be heard by children.

If staff or volunteers have a break time during their working hours, they may use their mobile phones during these times, but this must not be in an area where children are present.

In an emergency, staff needing to make a personal call during a lesson or whilst on duty should first obtain agreement from the Headteacher, ensure that adequate cover has been put in place and make the call in an area not used by children.

Staff must give the school telephone number to their next of kin in case it is necessary for the staff member to be contacted, in an emergency, during school working hours.

Camera or video functions on personal mobile phones must not be used in the school by staff to take images of children under any circumstances.

The school recognises that the use of mobile phones on school trips can be beneficial in ensuring safety for all members of the school party. The party leader should carry an office mobile phone for use in contacting other staff members or volunteers on the trip, contacting the school or contacting the emergency services. If the office mobile phone is unavailable then the party leader will seek permission from the Head teacher to take their personal device agreeing that they will follow the above protocol and only use the phone for emergency contact purposes.

Failure by staff to comply with the mobile phone policy guidelines could result in disciplinary action.

The school will advise visitors and parents/carers that mobile phones are not to be used in any areas accessible to pupils. This includes all uses phone calls, texting and photographing. If a visitor or parent/carer is seen using their mobile phone, they will be asked politely to desist from using it.

- **Acceptable Use Agreement**

All members of the school community are responsible for using the school IT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use agreements are revisited and re-signed annually at the start of each school year and amended accordingly in the light of new developments and discussions.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made.

All teachers have access to a school laptop and an assessment ipad that is used in school and at home. Secure systems are put in place to ensure that data is secure at all times. Spot checks are carried out on all devices throughout the year to ensure that they are used appropriately.

- **Misuse**

Issues related to E-Safety should be reported to the IT / Computing Co-ordinator OR Headteacher and it will be followed up accordingly. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

At Hollywater we seek to provide information and awareness to parents and carers through:

  - Letters and newsletters sent by hand or via email
  - School website
  - Parents evenings – virtually or in school

- Text messaging

- Reference to various resources and materials shared via email or text message

This document refers to and should be read in conjunction with :

- Acceptable Use agreements for staff and pupils
- Safeguarding policy
- Data Protection policy
- Privacy notices for staff, parents and pupils