Hollywater School

Inspire. Believe. Achieve.

E-Safety Policy

Approved by Chair of Governors, Silas Jones		**Date:** November 2023
Headteacher: Maria-Brigid Ryan		
Last reviewed on:	October 2022	
Next review due by: (Annually)	November 2024	

Purpose

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.

This E-Safety Policy outlines the commitment of Hollywater School to safeguard members of our school community online in accordance with statutory guidance and best practice. This E-Safety Policy applies to all members of the school community (including staff, learners, Governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Hollywater School will deal with such incidents within this policy and associated safeguarding and behaviour for learning policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

The purpose of this policy is to ensure that all children and young people at our school are able to use the internet and other online resources in a safe and responsible manner. This policy outlines the expectations for online behaviour, as well as the consequences of inappropriate use. We aim to:

Protect our vulnerable students: We recognise that some of our students may be more vulnerable to harm from online activities, and we are committed to taking all necessary measures to protect them.

Promote responsible use: We encourage our students to use the internet for educational purposes and to avoid any behaviour that could be considered inappropriate or illegal. We want to ensure that our students are able to use the internet in a way that is both safe and productive.

Raise awareness: We recognise that online safety is an ongoing concern, and we are committed to raising awareness about the potential risks and challenges of using the internet. We provide training and educational resources to our students, staff, and parents to ensure that everyone in our school community understands the importance of online safety.

Encourage parental involvement: We believe that parents play a vital role in promoting online safety, and we encourage all parents to become involved in monitoring their child's online activity and reporting any concerns or incidents to the school. We want to work together with parents to create a safe and supportive online environment for all of our students.

Overall, the purpose of this policy is to promote a culture of responsible and safe internet use in our school. We believe that by working together, we can create a safe and supportive online environment for all of our students.

The breadth of issues classified within E-safety is considerable, but can be categorised into four areas of risk as stated within Keeping Children Safe in Education:

> **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
>
> **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
>
> **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
>
> **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.
>
> (DfE Keeping Children Safe in Education 2023)

1. Development and Monitoring

Role	**Named Person**
E-Safety Coordinator	Sarah Kitching (DHT) / Maria-Brigid Ryan (HT)
Designated Safeguarding Lead	Sarah Kitching (DSL)
Deputy Designated Safeguarding Leads	Maria-Brigid Ryan, Helen West, Abi Appleton and Maria Butcher
IT and Network Manager	John Reed

This E-Safety policy has been developed by the IT (teaching and learning) Co-Ordinator and the Designated Safeguarding Lead in conjunction with the School Leadership team and the IT and
Network Manager. As part of this policy, records will be maintained on CPOMS of online safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

The school will monitor the impact of the policy using:

- Feedback from staff, pupils, parents / carers, governors
- Logs of reported incidents
- Internet activity monitoring logs from Agile

2. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness.

The Safeguarding Governor will also conduct regular online safety checks in relation to the school filtering and monitoring systems to ensure we are complying with elements of the KCSIE (2023).

Headteacher / Senior Leadership Team

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the IT Co-Ordinator and Designated Safeguarding Lead.

- The Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.

- The Headteacher / Senior Leadership Team are responsible for ensuring that the IT Co-ordinator/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their roles.

- The Headteacher / Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child / children, via any cloud-based website, Learning Platform or Gateway, have adequate information and guidance relating to the safe and appropriate use of this online facility – school privacy notices.

IT Coordinator & Designated Safeguarding Lead

The IT Coordinator & Designated Safeguarding Lead:

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school E-safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Report to the School Leadership Team serious breaches of E-Safety and related policies
- Provide training and advice for staff
- Liaise with the Local Authority
- Receive reports of online safety incidents and create a log of incidents to inform future safety developments
- Are trained in and share with staff an awareness and understanding of online safety issues and the potential for serious child protection issues that can arise from:
    - ✦ Sharing of personal data
    - ✦ Access to illegal / inappropriate materials
    - ✦ Inappropriate online contact with adults / strangers
    - ✦ Potential or actual incidents of grooming
    - ✦ Cyber-bullying
    - ✦ Sexting
    - ✦ Revenge pornography
    - ✦ Radicalisation (extreme views)
    - ✦ CSE

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current school online safety policy and practices
- They have read, understood and signed the E-Safety Policy and school Staff Acceptable Use Agreement (AUP)

- They report any suspected misuse or problem within CPOMS and to the IT Coordinator/ Designated Safeguarding Lead for investigation / action / sanction

- Digital communications with pupils and parents / carers (email / voice) should be on a professional level

- Students / pupils understand and follow, as appropriate for age and ability, the school E-Safety and pupil acceptable use agreement

- Students / pupils understand and follow E-Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour for learning and safeguarding policies.

- In lessons where internet use is planned students / 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.

- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT and Network Manager / Technical Staff

Responsible for ensuring that:

- they are aware of and follow the school E-Safety Policy

- the school technical infrastructure is secure and is not open to misuse or malicious attack

- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body (KCSIE)

- there is clear, safe, and managed control of user access to networks and devices

- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action

- the relevant filtering and monitoring systems are in place and regular checks are conducted to ensure their effectiveness

Pupils

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Agreement, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.

- will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyber-bullying etc.

- should understand that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local online safety campaigns / literature.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our safeguarding policies.

3. Education and Training Education – Pupils

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

Education – Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Letters, website, social media, newsletter articles
- Parents evenings

- Reference to external websites
- High profile events such as Internet Safety week
- Family learning opportunities
- Publishing the school E-Safety Policy on the school website

Education and Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school E- Safety and Acceptable Use policies.
- The IT Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required

Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

Filtering

- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering and KCSIE (2023).
- access to online content and services is managed for all users
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- filtering logs are regularly reviewed to check for breaches of the filtering policy, which are then acted upon.

- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The school protects users and school systems through the use of the appropriate blend of strategies. These include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network separated copies externally
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Manager (or other person) and will be reviewed, at least annually
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the IT Manager who will keep an up-to-date record of users and their usernames

- the master account passwords for the school systems are kept in a secure place, e.g. school safe. It is recommended that these are secured using two factor authentication for such accounts
- passwords should be complex and long
- records of learner usernames and passwords for learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for younger learners may be reduced and should not include special characters.
- password requirements for learners should increase as learners ability progresses
- The IT Manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed policy is in place (to be described) for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place (to be described) regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks) by users on school devices. These can be used but only if encrypted with bitlocker.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the data protection policy

4. Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet / social media. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on 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.

- Students / pupils must not take, use, share, publish or distribute images of others without their permission

- Written permission from parents or carers will be obtained when a pupil starts school before photographs of students/pupils are published on the school website or social media. This permission can be withdrawn at any time. Students' / Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs.

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

5. Use of 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.

6. Use of web based tools

Our school uses the public facing website, www.hollywaterschool.co.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 a secure web-based assessment tool 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.

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school's Data Protection Policy.

In summary, personal data will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must be aware that a breach of the Data Protection Act may result in the school or an individual fine

Staff must also ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- Access personal data on secure password protected computers and other devices or via any online Learning Platform or SMIS ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected.)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it is no longer required

8. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the E-Safety Coordinator – 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.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Individual email addresses will be provided to some pupils if deemed appropriate for their level of ability by their class teacher. These will be monitored by school.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer

- The school is not responsible for the loss, damage or theft of any personal mobile device

- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device

- Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites

9. Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material
- Criminally racist material
- Other criminal conduct, activity or materials

The incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

10. Monitoring and review

This policy will be reviewed annually, or earlier if necessary in line with national and/or local updates.