HOLY TRINITY PEWLEY DOWN

A Federation of Holy Trinity Junior & Pewley Down Infant Schools, Guildford

ON-LINE SAFETY POLICY

Should serious online safety incidents take place, the following external persons / agencies should be informed:	- **Local Area Designated Officer or** - **Police**

Opening Statement and Scope of the Policy

Holy Trinity Pewley Down School (HTPD) believes that the use of information technology (ICT) and the internet in schools enhances children's learning and forms an integral part of modern life. Recognising online safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications. At HTPD, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Through application of this policy, we hope to ensure that every child at HTPD is able to fully "embrace the future with hope and confidence" through safe and appropriate use of technology. Our approach is centred on our school motto of "Learn to Live".

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors & community users) who have access to and are users of school ICT systems, both in and out of the school.

The school's online safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Safeguarding.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

Aims

- To set out the roles and responsibilities of different members of the HTPD School community
- To outline the coverage and content of the HTPD e-safety curriculum taught to pupils
- To specify how the information contained within this policy is shared with all other members of the school community, including staff, parents, volunteers, visitors and community users
- To detail what constitutes acceptable use for each of these groups in a code of conduct
- To explain the process for dealing with breaches of the aforementioned code of conduct including instances of cyberbullying

Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the ECM Committee receiving regular information about online safety incidents

and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs
- reporting to ECM committee and full governing body when necessary

Headteacher & Senior Leadership Team

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be shared with the Online Safety Co-ordinator
- The Headteacher and (at least) 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. (see Appendix 3 - flow chart on dealing with online safety incidents)
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher 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 Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator

Online Safety Coordinator

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Communicates with parents and other members of the school community to keep up to date with the latest advice and developments
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets termly with Online Safety Governor to discuss current issues, review incident logs and filtering logs
- Attends relevant committee of Governors
- Reports regularly to Senior Leadership Team

Network Manager

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority other relevant body Online Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that 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

- that the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or Online Safety Coordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching & Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (See Appendix 1)
- they report any suspected misuse or problem to the Headteacher or Online Safety Coordinator for investigation
- all digital communications with pupils, parents/carers, other members of the school community and external agencies should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Pupil acceptable use policies (See Appendix 2)
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations at an age-appropriate level
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, 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

Designated Safeguarding Leads (DSL)

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- are responsible for using the school technology systems in accordance with the Pupil Acceptable Use Agreement (See Appendix 2)
- have an age-appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

E-Safety in the Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the

school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Policy (Appendix 2) and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education of Parents & 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 on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings including meet the team evenings and parent consultations
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training of 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. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements. It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.
- New developments in the field will be passed on to staff via 'Hot Topics' at the weekly briefing when required.

Use of Digital Images/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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images will usually only be taken on school equipment. On rare occasions, staff may feel it necessary to capture particular moments to support educational aims and find that their own personal device is the only one available. In such cases, the relevant media should be moved on to the school network as soon as possible and permanently deleted from the original device
- 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 without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Technical – Infrastructure, Equipment, Filtering & Monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 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 must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must 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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, 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, memory stick or any other removable media:
- the data must be encrypted and 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 (below) once it has been transferred or its use is complete

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In cases where suspected illegal activity has taken place, the flowchart for responding to incidents of misuse (see Appendix 3) should be followed.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

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, 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 actions described in detail in the relevant policies (Behaviour, Anti-Bullying & Staff Disciplinary)

Monitoring the Effectiveness of the Policy
Monitoring the effectiveness of this policy will be performed at least biannually by Tom Everard, Onlline Safety Co-ordinator, the Senior Leadership Team, ECM and James Peers, Network Manager.

Review
The Governing Body of HTPD first adopted this policy in 2012. It will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Date last reviewed: **January 2019**

Date for next review: **January 2020**

Mark Sharman
Governor of Holy Trinity Junior & Pewley Down Infant Schools
ECM Committee

Appendix 1

On-line Safety Policy – Staff Acceptable Use

Devices

- Staff will take responsibility for all activity that takes place whilst using a device logged on to the server.
- Any ICT problems/issues should be reported to the Network Manager or School Business Manager
- ICT devices should not be used for anything illegal
- The School reserves the right to monitor all staff devices and associated usage taking place on the school site and also any usage of school owned devices in any location in the world
- No software may be in installed on any school owned device without the consent of the Network Manager
- Staff will take responsibility for all activity that takes place under their own login on their device (whether owned by the school or personally)
- Passwords are to be kept confidential and changed when requested to do so
- Individually issued devices must not be used by non-school employees (see also the Staff Ipad Loan Agreement if applicable – Appendix 4)
- Devices may temporarily be left in a locked vehicle if locked away in the boot and out of sight. They should not be stored or left in a vehicle overnight.
- Staff must not attempt to disable or remove monitoring software on any machine.
- Staff must not attempt to disable or remove the virus checker software on any machine.

Storage/Printing

- Staff must be mindful of available space on the server and email storage and regularly clear out old and unwanted files.
- Printouts should be in black and white (where possible) and kept to a minimum.

Internet & Email Use

- Staff must assume responsibility for any sites visited, files downloaded, content viewed or emails received/sent using or on a school device/network.
- Staff must not attempt to bypass the schools filtering system by attempting to access proxy sites.
- The use of email/internet for the following reasons is forbidden:
    - betting and/or gambling
    - dating websites
    - personal financial gain
    - advertising purposes
    - political purposes
    - viewing / downloading of racist, pornographic, sexist, obscene or any other unsuitable material
    - posting of anonymous messages
    - sending libellous, slanderous, threatening or abusive messages
    - any illegal activities
- The copyright and intellectual property rights of all content viewed / downloaded must be respected.
- Staff should beware of emails and/or attachments from unknown sources. If in doubt, delete immediately. Do not open any suspicious message(s).
- The School accepts no liability for any personal financial transactions which are made across the internet/email.
- Where inappropriate sites are accessed by accident, the IT Manager should be informed immediately.
- Staff should note that emails can be as legally binding as a written letter.
- Non-required emails and attachments should be deleted once read.
- Nothing should be sent via email that could tarnish the School's name or expose it to legal action.
- The contents of any sent email must not infringe copyright.

E-Safety

- Personal Data – No personal data, including information relating to students, should ever be passed on to an unsecured third party individual or site.
- Social Networking Sites – Staff should not be 'friends' with any pupils or ex-pupils who are under the age of 18 when using social networking sites (e.g. Facebook).
- Images – Staff may only take images of pupils for official school purposes. – Images of pupils (i.e. trips, visits, events, etc.) must only be stored on the school network. Any images captured on personal devices must be moved (e.g. by email) to the server as soon as practicable so that they can be stored securely. Images of pupils should be deleted after the pupil has left.
- Contact Details – Staff should be cautious in giving out contact details and should never give their personal email address to a parent or pupil.
- Emailing parents – Emails to parents must only be made using school email accounts. Staff should not email pupils directly.
- Conduct – Staff should be cautious when using social media to ensure that their profiles are sufficiently secure and that any media posted by them does not bring the reputation of themselves or the school into disrepute.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Breach of Staff Acceptable Use Policy

Any breach of the Staff Acceptable Use Policy may be deemed as misconduct and dealt with in accordance with the School's Disciplinary Policy.

I understand and agree to abide by the above Staff Acceptable Use Policy

Staff Name (Please Print) ……

Staff Signature ……..……..

Date ……

Appendix 2

Safe use of the internet – a guide for HTPD pupils

This appendix should be adapted by each year group to ensure that it is appropriate to the age group and its needs. A child friendly version should be displayed in each classroom for children to refer to.

Each year group should cover the points mentioned in this Appendix in an age-appropriate manner.

School computers

- Pupils must accept responsibility for all activity that takes place under their own network login.
- Pupils may only use their own network accounts.
- School computers must only be used for school business and must not be used for any illegal, obscene, offensive, profit making or commercial purpose.
- Pupils should be aware that the School is able to monitor all computers, devices and what they are being used for both at school and any usage of school owned devices in any location in the world.
- No software may be in installed on any school owned device by pupils.
- Passwords must be kept confidential and changed when requested to do so.
- Pupils must not alter any of the settings on school owned devices.
- Any ICT problems/issues should be reported to the teacher immediately.

Internet & Email

- School internet must only be used for school related work.
- Emails should be sent/received using a school registered account only. Access to hotmail and other internet based email accounts is forbidden.
- The copyright and intellectual property rights of all content viewed / downloaded must be respected.
- Emails and/or attachments from unknown/suspicious sources should not be opened and should be deleted immediately.
- Non-required emails and attachments should be deleted once read.
- Where inappropriate sites are accessed by accident the teacher should be informed immediately.

E-Safety Guidance

- Personal data should never be passed on to anyone.
- Pupils should never agree to meet people they have met on-line.
- Access to social networking/chat room sites is not permitted in school.
- Photos of staff and students must not be labelled and/or copied from the school network.
- Pupils must not pass on anyone else's contact details without permission.

Appendix 3

Flowchart for Responding to Incidents of Misuse