Holy Trinity CE Primary School

Mission Statement – 'Growing and learning in Christ through faith, family and friendship'

Online Safety Policy

Contents

Introduction

Online safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

This Online Safety Policy is part of our safeguarding procedures and operates in conjunction with other policies including those for Pupil Behaviour, discipline and exclusions, Anti-bullying and Child Protection.

Our Online Safety Policy has been written by the school, building on the Lancashire Children and Young Peoples' Directorate and Government guidance. It has been agreed by Holy Trinity's teaching staff team and approved by the Governing Body.

The school online safety coordinator is: Mrs Jennifer Stevenson.

The responsible member of the Governing Body is: Mrs Kath Gillam.

Scope of the Policy

This policy applies to all members of Holy Trinity CE Primary School (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of the school. The school will deal with any online safety incidents detailed within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Mrs Kath Gillam has taken on the role of the online safety Governor. The role of the online safety Governor will include regular meetings with the Computing subject leader and reporting to relevant Governors.

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. 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.

Computing Subject Leader

The Computing subject leader takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents. They should ensure:

- 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
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- they receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- they meet regularly with the online safety Governor to discuss current issues and developments

Teaching and Support Staff

All teaching and 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 (AUP)
- they report any suspected misuse or problem to the Headteacher and Computing subject leader for investigation
- all digital communications with pupils/parents/carers 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

Designated Safeguarding Lead

DSL - Mrs. S Smith

Back –up DSL – Mrs. A Whitaker

The 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

Pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. They 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.

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, the school website and information about national/local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Policy Statements

Education of Pupils

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 is a focus in all areas of the curriculum and staff 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 is provided as part of Computing and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies or themed weeks
- Pupils 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.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school.
- 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.

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:

- Newsletters and the school web site
- Parents/Carers sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Education and Training of Staff/Volunteers

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:

- All new staff should receive information regarding online safety as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Computing subject leader will receive regular updates by reviewing guidance documents released by relevant organisations.

Education and Training of Governors

Governors should take part in online safety training/awareness sessions. This may be offered by:

- Attendance at training provided by the Local Authority
- Participation in school training/information sessions for staff or parents (including assemblies and online safety lessons)

Technical- infrastructure/equipment, filtering and 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.

- 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.
- Teaching staff will be provided with a username and secure password by the ICT subject leader 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 and Computing subject leader and kept in a secure place.
- The Computing subject leader 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.

Use of Digital and Video Images

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.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. 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/local press. Permission is gained from parents and carers when the child is admitted to School; it is the responsibility of parents to inform us if there are any changes that may necessitate removal of permission.
- Staff and volunteers can take digital/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 taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Sensitivity must be used when displaying photographs of children e.g. considering the angle of shots for children engaged in PE activities. Under no circumstances must any photographs of children be taken when: changing for PE, in children's toilets and cloakroom areas.
- 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. The press have special permissions in terms of data protection and may wish to name individual children to accompany a photograph. Parents are made aware of this in the use of images procedures.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and can be monitored.

- Users must immediately report to the headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents/carers (email, blogs etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used by pupils for educational use as required within the curriculum
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Mobile Technology

Mobile technology devices used in school must be school owned/provided and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. All users should understand that the primary purpose of the use of mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme. The school Acceptable Use Agreements for staff, pupils and parents/carers considers the use of mobile technologies.

The following procedures relate to the use of personal mobile phones in school:

- Staff may bring personal mobile phones on to the School premises but these should be switched off or on silent during the School day.
- Staff may check their mobile phones in the staffroom at break time or lunchtimes. Phones should not be used under any circumstances in classrooms when children are present.
- If staff are anticipating they may need contacting during the School day they should give the School telephone number to the individual who may need to contact them and office staff will notify and get the staff member should that need occur. Only in exceptional circumstances may staff mobile phones be left on in classrooms and the Head Teacher must give permission for this.
- Staff will be given permission to use mobile phones in situations where contact with the main School is advisable and a risk assessment has been undertaken e.g. educational visits, activities on the school field or in the school community room.
- Staff mobile phones must be stored away from pupils during the day/lockers are available
- It is a disciplinary breach to use a mobile phone in a classroom during school hours or when children are present e.g. during after school clubs
- Staff should not take any images of children on personal mobile phones.
- Any breach of these procedures may result in disciplinary proceedings and the governing body being informed. If a staff member suspects any other member of the staff misusing a mobile device the Head teacher must be informed immediately.
- In accordance with the School rules, mobile phones must not be brought in to School by pupils. If a parent contacts School and has a valid reason why their child needs a mobile phone on a particular day, the Head teacher must be informed and the phone taken to the School office until the end of the School day for safe keeping.

Social Media- Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly, for acts of their employees during their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly by the Computing subject leader and head teacher to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Publishing Material on the School Website

The school will maintain editorial responsibility for the school initiated web site to ensure that content is accurate and quality of presentation is maintained.

- The school will maintain the integrity of the school web site by ensuring that responsibility for uploading material is never handed over to pupils and that passwords are protected.
- The website will comply with the school's guidelines for publications.
- The point of contact on the website will be the school address, e-mail and telephone number. Home information or individuals' e-mail addresses will not be published.
- School will obtain permission from parents for the use of pupils' photographs. Permission is gained from parents and carers when the child is admitted to School; it is the responsibility of parents to inform us if there are any changes that may necessitate removal of permission.
- Group photographs should not have a name list attached. Identities of pupils must be protected at all times and parents may be consulted about publishing work from pupils.

Data Protection

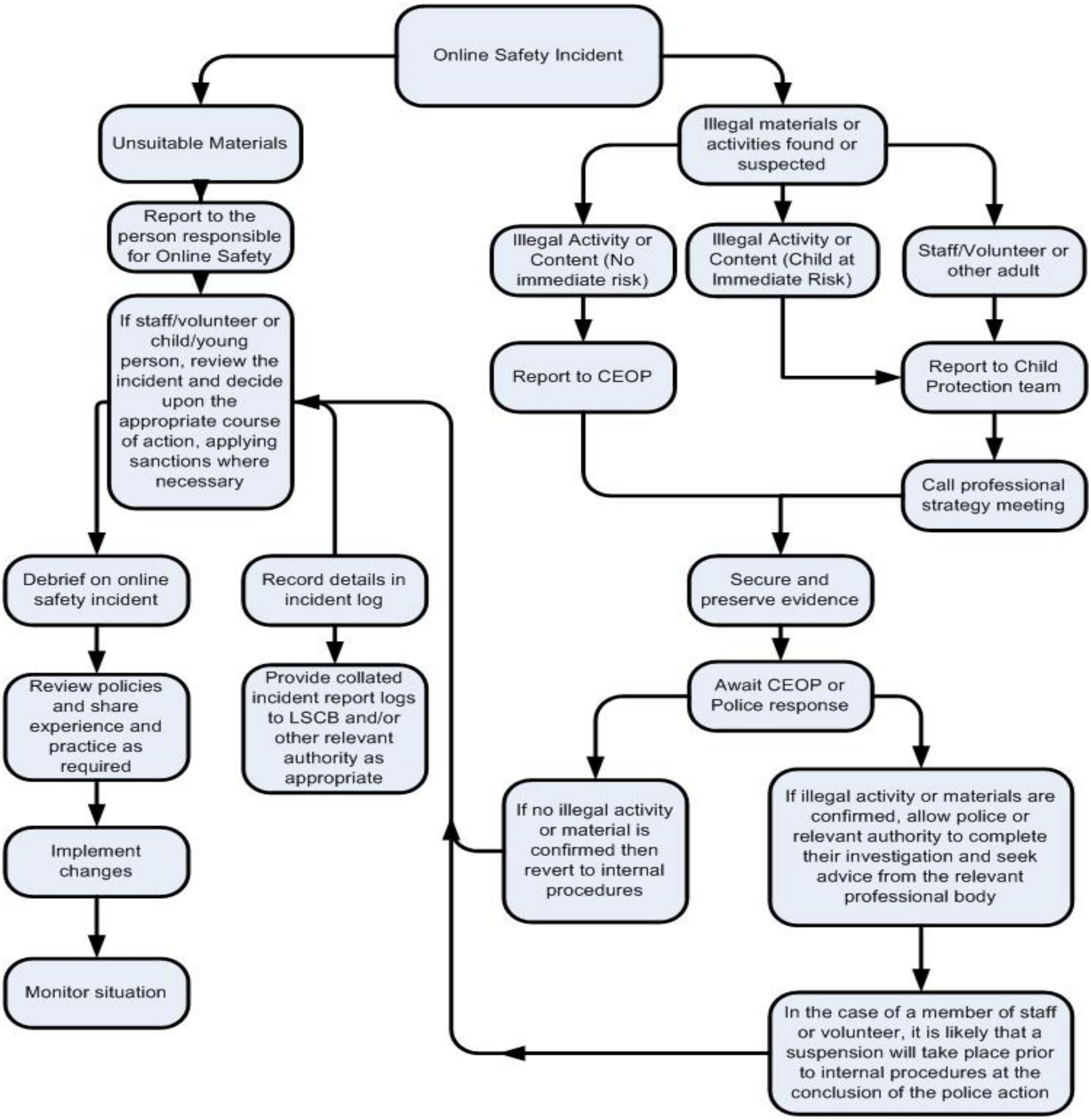
Personal data will be recorded, processed, transferred and made available according
to the Data Protection Act 1998.
Staff must ensure that they:

- 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.

Dealing with Online Safety Incidents

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

School Actions and Sanctions

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 normal behaviour / disciplinary procedures as follows:

- Any complaints or breaches of conduct will be dealt with promptly and recorded on the incident sheet.
- Responsibility for handling incidents will be given to a senior member of staff (Head Teacher/Assistant Head Teacher)
- Pupils and parents will be informed of the procedure
- Parents and pupils will need to work in partnership with staff to resolve any issues arising

- The facts of the case will need to be established, for instance to ascertain whether the issue has arisen through home Internet and e-mail use or through contacts outside school
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies
- Sanctions for irresponsible use will be linked to the school's Behaviour Policy and will consist of the following actions depending on circumstances:
  - Discussion with Class teacher/Head Teacher
  - Letter home /discussion to inform parent or carer
  - Further consequences such as withdrawal of Internet and e-mail privileges depending on circumstances

Development of this Policy

This Online Safety policy has been developed and agreed by:

- Headteacher/Senior Leaders
- Computing Subject Leader
- Staff – including Teachers and Support Staff
- Governors
- Pupils
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review of this Policy

This Online Safety policy was approved by the Governing Body on:	February 19th 2018
The implementation of this Online Safety policy will be monitored by the:	Headteacher: Mrs Sally Smith Computing Subject Leader: Mrs Jennifer Stevenson
Monitoring will take place at regular intervals:	Ongoing
The Online Safety Policy will be reviewed 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. The next anticipated review date will be:	Spring Term 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Questionnaires of
  - pupils
  - parents / carers
  - staff