The Holy Trinity C of E Secondary School

Online-Safety Policy – draft under review		
Policy last reviewed:	March 2023	
Next review due:	September 2023	
Member of staff responsible:	Kate Bramley	
FGB Approved (if applicable)	Not applicable	

Vision Statement
Our vision is to be a centre of excellence for learning inspired by Christian values where young people fulfil their potential.

Mission Statement:
Deeply Christian, open to all.

Values Statement
Holy Trinity school aims to serve its community by providing an education of the highest quality within the context of Christian belief and practice. It encourages an understanding of the meaning and significance of faith, and promotes Christian values through the experience it offers to all its students.

Dignity
Underpinning all that we do is the core belief in the ultimate worth of each person as a child of God – precious, valued and loved by God. Dignity comes from the knowledge of our ultimate worth as human beings.

Community
Having understood our value as individual human beings, we express this value through the quality of the relationships that we share with each other. Community, living well together, is of very great importance to us as a school, as is the place we each take in the wider community locally, nationally and internationally.

Wisdom
As a school we seek to foster confidence, delight and discipline in seeking wisdom, knowledge and truth. This is achieved through the nurturing of academic habits and skills, emotional intelligence, resilience and creativity across the breadth of the curriculum.

Hope
As we prepare our students for the future we look to open up horizons of hope and aspiration, encouraging our students to embrace these with confidence and sending them out to make a difference to the world in which they live.

Contents

Online Safety Policy

This policy applies to all members of Holy Trinity school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of Holy Trinity school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off Holy Trinity school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of Holy Trinity school, but is linked to membership of Holy Trinity school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Holy Trinity School will deal with such incidents 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

The following section outlines the online safety roles and responsibilities of individuals and groups within Holy Trinity 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 *Governors* 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 alongside the role of the* Safeguarding Governor. The role includes:

- regular meetings with the Online Safety Lead (also the Designated Safeguarding Lead)
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- 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 Holy Trinity school community, though the day to day responsibility for online

safety will be delegated to the *Online Safety Lead who is also the Designated Safeguarding Lead* and a member of the Senior Leadership team

- The Headteacher and Online Safety Lead are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority* procedures).
- *The Headteacher is responsible for ensuring that the Online Safety Lead 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 support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Online Safety Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing Holy Trinity 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
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of *Governors*
- reports regularly to Senior Leadership Team

Incidents are dealt with in line with procedure laid out in the Behaviour and Discipline Policy.

Network Manager / Technical staff

The Network Manager / Technical Staff is responsible for ensuring:

- that Holy Trinity school's technical infrastructure is secure and is not open to misuse or malicious attack

- that Holy Trinity school meets required online safety technical requirements and any *Local Authority* 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

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 *Online Safety Lead* for investigation / action / sanction
- all digital communications with students / 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
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned students 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 Lead / Online Safety Lead

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
- online-bullying

Students:

- are responsible for using Holy Trinity school digital technology systems in accordance with the Student Acceptable Use Agreement

- have a good 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Holy Trinity school's Online Safety Policy covers their actions out of school, if related to their membership of Holy Trinity 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. Holy Trinity school will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support Holy Trinity school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student records
- *their children's personal devices in Holy Trinity school (where this is allowed)*

Community Users

Community Users who access school / website / Learning Platform as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in online safety / digital literacy is therefore an essential part of Holy Trinity school's online safety provision. Children and young people need the help and support of Holy Trinity 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 is provided as part of Computing / REACH / other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students are 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.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are 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.
- *Students are helped to understand the need for the student Acceptable Use Agreement 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, best practice is followed and students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *In lessons where students are allowed to freely search the internet, staff are 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 (e.g. 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 – Parents / Carers

Many parents and carers may 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 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.

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

- *Letters, newsletters, web site, Learning Platform*
- *Parents / Carers evenings / sessions*
- *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 – 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:

- 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 Holy Trinity school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events 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 / team meetings / INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors take part in online safety training / awareness sessions, with particular importance for those who are members involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority National Governors Association / or other relevant organisation.
- Participation in school information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems are managed in ways that ensure that Holy Trinity school meets recommended technical requirements
- There are 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 have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password by 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 and will be required to change their password every (90 days).
- The "master / administrator" passwords for Holy Trinity school ICT systems, used by the Network Manager (or other person) are also available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- 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 (child sexual abuse images) 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. There is a clear process in place to deal with requests for filtering changes
- Internet filtering / monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.
- Holy Trinity school has provided enhanced / differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on Holy Trinity school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Any actual / potential technical incident / security breach are reported to the DSL or Safeguarding Manager.
- 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 Holy Trinity school systems and data. These are tested regularly. Holy Trinity school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off Holy Trinity school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising Holy Trinity school's wireless network. The device then has access to the wider internet which may

include Holy Trinity school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour and Discipline Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of Holy Trinity school's Online Safety education programme.

- Holy Trinity school Acceptable Use Agreements for staff, students and parents / carers will give consideration to the use of mobile technologies
- Holy Trinity school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
No network access	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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. Holy Trinity school will

[1] Authorised device – purchased by the student/family. This device may be given full access to the network as if it were owned by the school.

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 students 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 students are published on Holy Trinity 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* in the digital / video images.
- Staff and volunteers are allowed to 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.
- should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or Holy Trinity school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website Care or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Holy Trinity school ensures that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Lead (DPO).
- 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.

- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- Holy Trinity school has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff 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 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 (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how Holy Trinity school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Students			
Communication Technologies		ain times	ected staff		ed off and in bag	ain times	:aff permission	
Mobile phones may be brought to Holy Trinity school	✓				✓			
Use of mobile phones in lessons			✓				✓	
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices			✓					✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓
Use of social media				✓				✓
Use of blogs				✓				✓

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

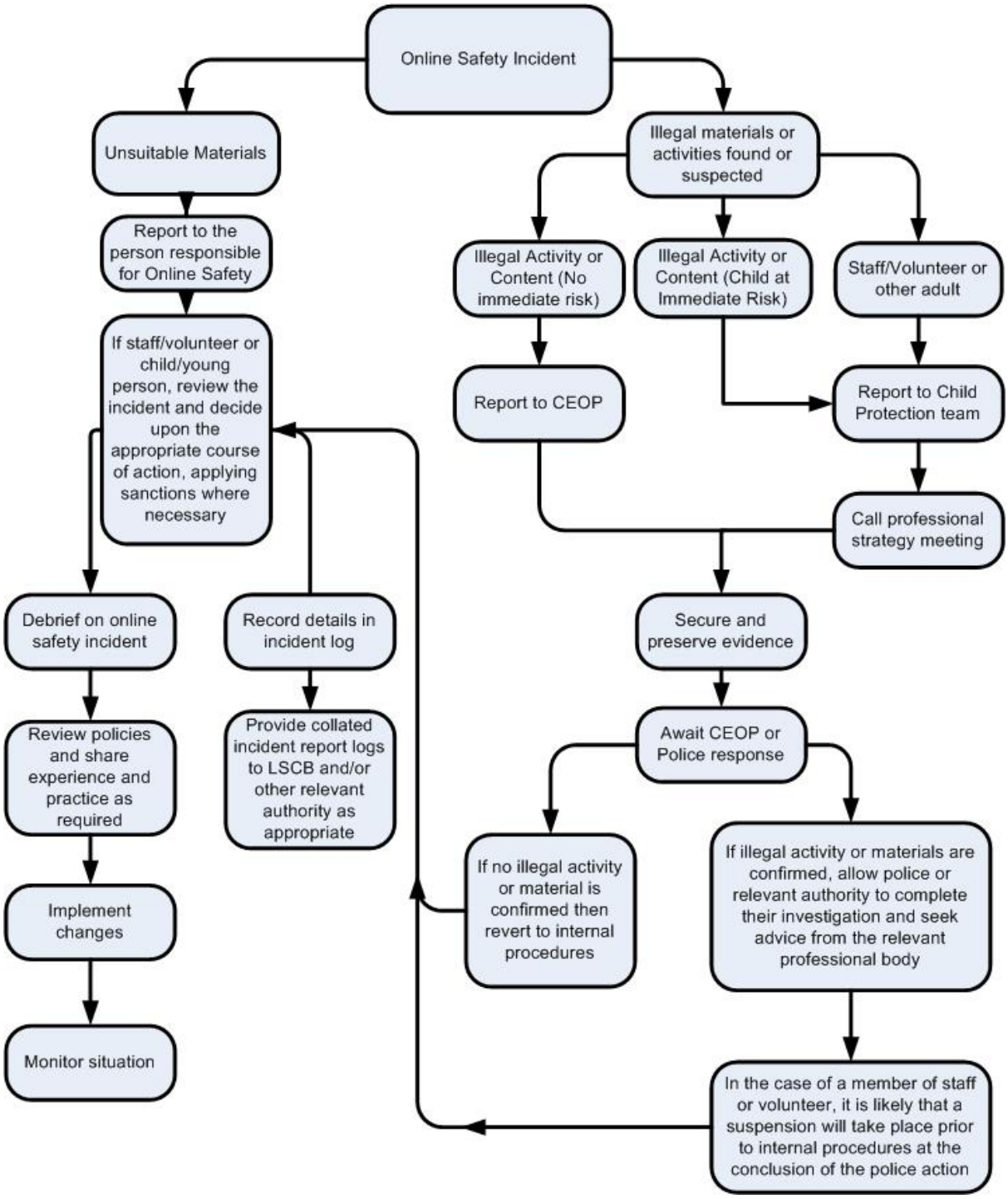
- The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with Holy Trinity school policy, the receipt of any communication that makes 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 students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

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 (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of Holy Trinity 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 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 Holy Trinity 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.

Appendices

School Technical Security Policy

Technical Security

Policy statements

Holy Trinity school will be responsible for ensuring that Holy Trinity school infrastructure / 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 receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that Holy Trinity 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
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of Holy Trinity school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will 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 Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for Holy Trinity school systems, used by the technical staff must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts

Staff Passwords

- All staff users will be provided with a username and password
- All users will be provided with a username and password

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that Holy Trinity school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of Holy Trinity school's filtering policy will be held by the Network Manager. They will manage Holy Trinity school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to Holy Trinity school filtering service must

- be logged in change control logs
- be reported to a second responsible person, who is the Designated Safeguarding Lead/Online Safeguarding Lead

All users have a responsibility to report immediately to (Peter Fallon) any infringements of Holy Trinity school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by Holy Trinity school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts Holy Trinity school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the

filtering system. Where personal mobile devices are allowed internet access through Holy Trinity school network, filtering will be applied that is consistent with school practice.

- Holy Trinity school manages its own filtering service
- Holy Trinity school has provided enhanced / differentiated user-level filtering through the use of the (Smoothwall) filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / students / students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that access Holy Trinity school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on Holy Trinity school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff and the Designated Safeguarding Lead. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of Holy Trinity school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Electronic Devices - Searching & Deletion Policy

Introduction

The changing face of information technologies and ever increasing student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search students in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that Holy Trinity school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide Holy Trinity school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under Holy Trinity school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under Holy Trinity school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by Holy Trinity school rules may only be searched for under these new powers if it has been identified in Holy Trinity school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under Holy Trinity school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break Holy Trinity school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The *Head Teacher* must publicise Holy Trinity school behaviour policy, in writing, to staff, parents / carers and students at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006

- Education Act 2011 Part 2 (Discipline)
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

Training / Awareness

Members of staff should be made aware of Holy Trinity school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on Holy Trinity school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

Holy Trinity school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

S*tudents are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by Holy Trinity school.*

Authorised staff have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break Holy Trinity school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in Holy Trinity school rules as an item which is banned and may be searched for

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a *student / pupil* is in possession of a prohibited item i.e. an item banned by Holy Trinity school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the *student* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student/ pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *student* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that** serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:
The person conducting the search may not require the *student* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves). Staff will take account of Holy Trinity school's policy regarding religious garments / headwear

'Possessions' means any goods over which the *student* has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the *student / pupil* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under Holy Trinity school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave Holy Trinity school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices

Audit / Monitoring / Reporting / Review

The Online Safety Lead will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the DSL (Online Safety Lead / Online Safety Governor) at regular intervals alongside Safeguarding visits.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Mobile Technologies Policy (inc. BYOD/BYOT – Bring Your Own Device)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising Holy Trinity school's wireless network. The device then has access to the wider internet which may include Holy Trinity school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high-tech world in which they will live, learn and work.

For further reading, please refer to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/advice/bring-your-own-device-byod

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased

network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before Holy Trinity school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- Holy Trinity school Acceptable Use Agreements for staff, students/students and parents/carers will give consideration to the use of mobile technologies

- Holy Trinity school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete / amend as appropriate):
    - All school devices are controlled though the use of Mobile Device Management software
    - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
    - Holy Trinity school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
    - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
    - Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
    - *All school devices are subject to routine monitoring*
    - Pro-active monitoring has been implemented to monitor activity
- When personal devices are permitted:
    - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
    - Personal devices are brought into Holy Trinity school entirely at the risk of the owner and the decision to bring the device in to Holy Trinity school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
    - Holy Trinity school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by Holy Trinity school (Holy Trinity school recommends insurance is purchased to cover that device whilst out of the home)

- Holy Trinity school accepts no responsibility for any malfunction of a device due to changes made to the device while on Holy Trinity school network or whilst resolving any connectivity issues
- Holy Trinity school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around Holy Trinity school. Pass-codes or PINs should be set on personal devices to aid security
- Holy Trinity school is not responsible for the day to day maintenance or upkeep of the users' personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
  - Devices may not be used in tests or exams
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in school
  - Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during Holy Trinity school day
  - Devices must be in silent mode on Holy Trinity school site and on school buses
  - School devices are provided to support learning.
  - Confiscation and searching (England) - Holy Trinity school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
  - The software / apps originally installed by Holy Trinity school must remain on Holy Trinity school owned device in usable condition and be easily accessible at all times. From time to time Holy Trinity school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
  - Holy Trinity school will ensure that school devices contain the necessary apps for school work. Apps added by Holy Trinity school will remain the property of Holy Trinity school and will not be accessible to students on authorised devices once they leave Holy Trinity school roll.

- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Printing from personal devices will not be possible

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Holy Trinity school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *Holy Trinity school*, its staff, parents, carers and children.

Scope

This policy is subject to Holy Trinity school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent Holy Trinity school.
- Applies to such online communications posted at any time and from anywhere.

Professional communications are those made through official channels, posted on a school account or using Holy Trinity school name. All professional communications are within the scope of this policy.

Organisational control

Monitoring
School accounts must be monitored regularly and frequently

Behaviour

- Holy Trinity school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

- Digital communications by staff must be professional and respectful at all times and in accordance with this policy.
- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with Holy Trinity school's digital and video images policy.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts

- Students
    - Staff are not permitted to follow or engage with current or prior students/students of Holy Trinity school on any personal social media network account.
- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.

- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- Holy Trinity school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. Youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct

causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In Holy Trinity school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. Holy Trinity school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / students when they are off Holy Trinity school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/studentsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

Holy Trinity school Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

Safer Internet Centre – https://www.saferinternet.org.uk/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Internet Watch Foundation - https://www.iwf.org.uk/

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - http://www.netsmartz.org/

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

https://digital-literacy.org.uk/

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education
UK Safer Internet Centre Professionals Online Safety Helpline
https://cscp.org.uk/wp-content/uploads/2021/03/Guidance-for-safer-working-practice-for-adults-who-work-with-children-and-young-people-DCSF.pdf

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring
NEN – Advice and Guidance Notes

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
NCA – Cyber Prevent
Childnet – Trust Me