Online Safety Policy

Development / Monitoring / Review of this Policy

The Online Safety Policy has been developed by the Online Safety Committee made up of:

- Headteacher & Senior Leadership Team
- Online Safety Coordinator
- Teaching Staff
- E-safety Governor

Consultation has taken place through a range of formal and informal meetings

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on	*January 2018*
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Coordinator* *Senior Management Team* *Online Safety Governor*
Monitoring will take place at regular intervals:	*Annually (see monitoring timetable)*
The Online Safety Policy will be reviewed 3 yearly or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*January 2019*
Should serious online safety incidents take place, the following external persons / agencies should be informed as appropriate:	*Headteacher* *LADO* *Designated Safeguard Lead* *First Response*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Surveys / questionnaires of

- students / pupils
- parents / carers
- staff

Scope of the Policy

This policy applies to all members of The Trinity Federation schools (including staff, students / pupils, volunteers, parents / carers, visitors, community users and governors) who have access to and are users of school ICT systems, both on and off the premises.

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

Governors:

The Trinity Federation of 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 Online Safety Governor who will receive annual information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- annual meetings with the Online Safety Co-ordinators for each Trinity Federation school
- attendance at Online Safety Group meetings
- monitoring of online safety incident logs
- providing feedback at full governors meetings.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.

- The Headteacher and (at least) another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart).

- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Senior Leadership Team will receive regular monitoring reports from either the Online Safety Co-ordinator or the designated person for online monitoring.

Online Safety Coordinator:

- leads the Online Safety within school
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets annually with Online Safety *Governor* to discuss current issues and review incident logs
- attends relevant governors subcommittee meetings if required
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network is responsible for ensuring:

- **that** The Trinity Federation of **schools' technical infrastructure is secure and is not open to misuse or malicious attack**

- **that the** The Trinity Federation of **schools' meets required online safety technical requirements and any Local Authority Guidance that may apply.**
- **that** The Trinity Federation **users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Online Safety Coordinator for investigation.
- that monitoring systems are implemented and updated as agreed.
- That they work within the guidelines set out for data protection (GDPR 2018)

Teaching and Support Staff

The Trinity Federation of teachers 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 / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher, Senior Management Team or Online Safety Coordinator for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems and complying to the Staff Code of Conduct.
- online safety issues are embedded in all aspects of the curriculum and other activities
- Enable pupils to understand and follow the Online Safety Policy and acceptable use policies
- Enable pupils to 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~~ School and Federation policies with regard to these devices

- in lessons where internet is used ~~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

The Trinity Federation Designated Safeguarding Lead / Designated Person

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

The Trinity Federation Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil 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
- Must not share passwords with other pupils or staff
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers of the children in The Trinity Federation play a crucial role in ensuring that their children understand the need to use the internet devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, letters, school newsletters, email updates, school website or e-safety workshops.* 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
- social media
- their children's personal devices in the school

Policy Statements

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

- A planned online safety curriculum should be provided as part of Computing and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

- Pupils should be helped to understand the need for the Pupil Acceptable Use 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 is used, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and a record kept by the Online Safety Co-ordinator.

Education – Parents / Carers

Many Trinity Federation parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities

- Letters/newsletters

- High profile campaigns such as 'Safer Internet Day'

- Reference to the relevant websites and information via school website

- Online safety workshop

Education – The Wider Community

The Trinity Federation of schools may provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- *Online safety information may be accessible to a wide audience and not just be aimed at parents*
- *The school website may provide online safety information for the wider community*

Education & Training – Staff / Volunteers

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

- Regular 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 a copy of the Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings
- The Online Safety Coordinator will provide advice, training and guidance to individuals as required.

Training – Governors

The Trinity Federation Governors should take part in online safety training sessions, with particular importance for those responsibly for safeguarding and Online Safety. This may be offered in a number of ways:

- Attendance at training provided by external providers or National Governors Association

- Participation in school training sessions for staff, parents or participation in activities aimed at children

Technical – infrastructure / equipment, filtering and monitoring

The Trinity Federation of schools will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the designated people for online safety both internal and external will be effective in carrying out their online safety responsibilities on behalf of The Trinity Federation of schools:

- 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.

- Each school within the Trinity Federation of schools will ~~be~~ provide individual username and passwords as deemed appropriate by the Computing Coordinator. They will keep a secure, 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 100 days.

- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or Computing Coordinator and kept in a secure place.

- Staffordshire Learning Technologies 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The Trinity Federation of schools provide differentiated user-level filtering to ensure that only age-appropriate content is accessible to them

- The Headteacher or Office Manager regularly uses ~~PCE~~ monitoring software to monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement

- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. All incidents are reported to the class teacher, who would report to the Online Safety Coordinator for investigation.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly by Staffordshire Learning Technologies. The school infrastructure and individual workstations are protected by up to date virus software.

- Supply teachers, guests and trainees are allowed limited access to school systems via a 'supply' user in order to protect data and pupil information; their use is monitored using PCE software.

- An agreed acceptable use policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.

- Removable devices may only be used by pupils if permission is given by teaching staff

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

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

All users should understand that the primary purpose of mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Trinity Federation **schools'** Online Safety education programmes.

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

- The school allows:

	School Devices			Personal Devices (inc phone)		
	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	NO* (See below)	YES	YES
Full network access	Yes	Yes	Yes	NO	NO	NO
Internet only	YES	YES	YES	NO	YES	YES

- In special circumstances, the school may grant permission for a child to bring a mobile device on to the school premises. The mobile device must be securely stored in the school office and supervised use only is permitted.

Use of digital and video images in The Trinity Federation

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

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

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press, alongside the data protection guidelines (GDPR 2018).

- 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 is 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 pupils in the digital / video images.

- The Trinity Federation 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.

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

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

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

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 ~~1998~~ which states that personal data must be:

- Fairly and lawfully processed

- Processed for purpose that the consent was given

- Adequate, relevant and not excessive

- Accurate

- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Meeting the security regulations of GDPR 2018
- Only transferred to others with encrypted protection.

The Trinity Federation of schools must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It will follow the data protection guidelines set out in GDPR 2018.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Data processors, Data Controller and Data protection Officer
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

The Trinity Federation staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must 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.

The Trinity Federation Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. When using communication technologies the Trinity Federation schools considers the following as good practice:

- The official school service may be regarded as safe and secure. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the 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 pupils or parents / carers via email and school text messages must be professional in tone and content.

- 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.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The Trinity Federation schools provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the schools 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

- Risk assessment, including legal risk

Trinity Federation 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

When official school social media accounts are established they should be:

- *Approved by a member of the Senior Leadership Team*

- *Regular monitored by a member of the Senior Leadership Team or Online safety Co-ordinator*

- *A code of behaviour for users of the accounts, including how to deal with misuse or report issues*

Personal Use:

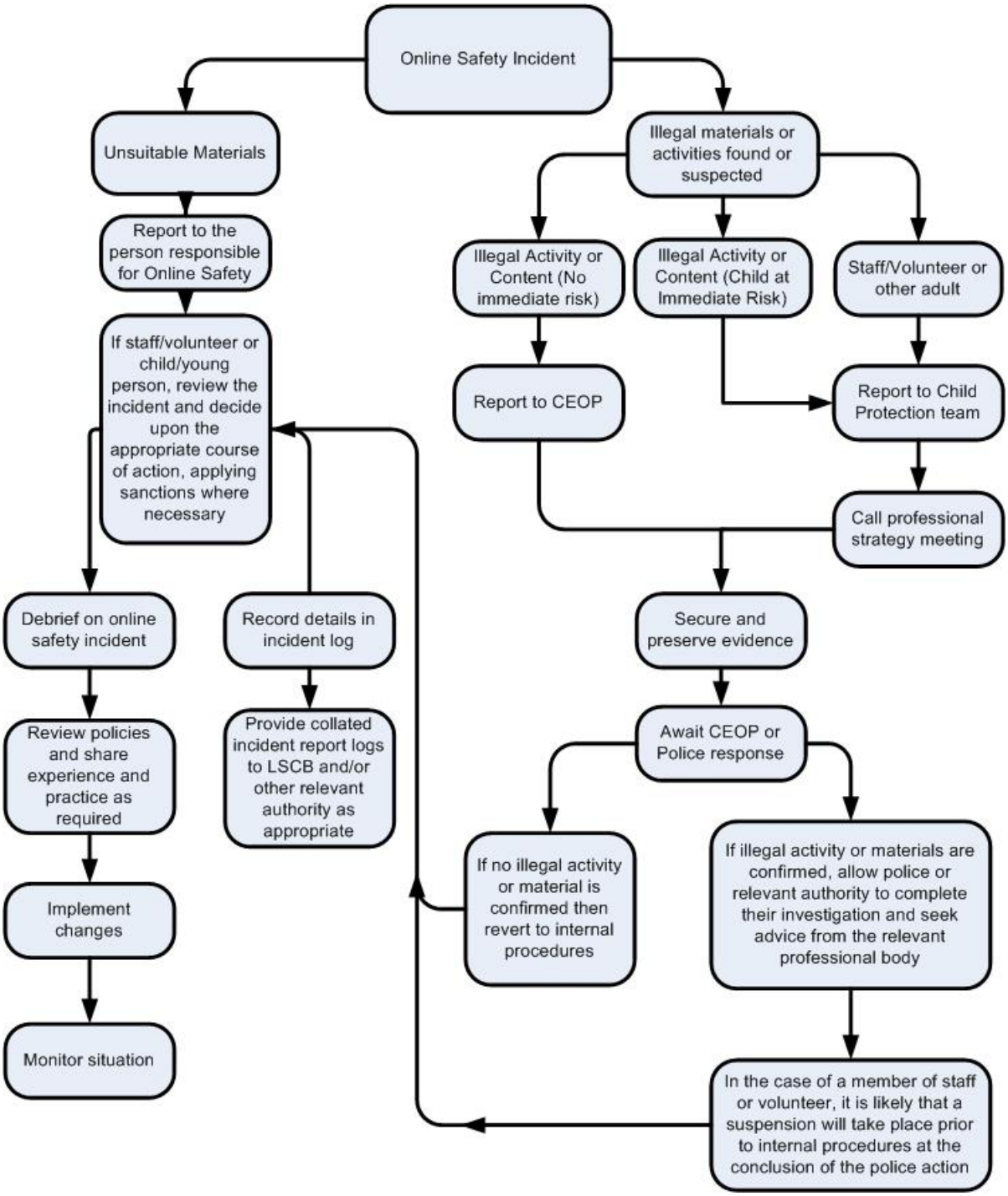
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process
- The *school's* use of social media for professional purposes will be checked regularly by the Online Safety Officer to ensure compliance with the school policies.

Responding to incidents of misuse

All Online Safety incidents will be dealt with as shown on flow diagram below:



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow The Trinity Federation of schools 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.
- Request the support of LADO to 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 Group or local organisation
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act

- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & 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. Depending on the nature of the incident, the school may take/ issue any of the following actions/sanctions.

- Refer to Class Teacher/ Headteacher
- Refer to technical support staff for filtering/ increased security measures
- Informing parents of incident
- Refer to Local Authority/Police
- Issue a 'warning'
- Removal of access to school systems
- Further school sanctions such as detention.

The above actions/sanctions would depend on the seriousness of the online safety incident, whether or not it was deliberate or accidental and also on whether the incident was involving a pupil, member of staff or someone within the wider school community. Therefore decisions on sanctions will be a 'case by case' basis.