Christ Church Primary School

Online Safety Policy

Background / Rationale

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our school online safety policy will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child’s education from the Headteacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside Christ Church Primary School. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Being exposed to extremist content and the risk of radicalisation.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
The new Counter-Terrorism and Security Act 2015 obliges schools (and other authorities) to prevent people from being drawn into terrorism including online and we therefore must put procedures in place to ensure that staff can deal with these situations.

Christ Church Primary School must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Curriculum and Standards Committee and the Computing/Online Safety Leader

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	December 2017
The implementation of this Online Safety policy will be monitored by:	The Computing/Online Safety Leader and the link Governor for Computing/Online Safety
Monitoring will take place at regular intervals:	termly
Christ Church Primary School will monitor the impact of the policy using:	• Logs of reported incidents taken from Futures Cloud or reported by staff. • Internal monitoring data for network activity.
The Curriculum and Standards Committee will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Leaders/Group at regular intervals:	At least once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	December 2018
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Designated safeguarding Officer – Headteacher, LA Safeguarding Officer, LADO, Police

Scope of the Policy

This policy applies to all members of the Christ Church Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of school. At Christ Church we regard online safety as a wider community issue and confirm that we will deal sensitively with our school online safety incidents that relate to members of the school community and with regards to staff in line with the AUP.

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 Christ Church Primary School and affects their education whilst at school. This may involve outside agencies to support the school in dealing with the issue appropriately.

Christ Church Primary 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 Christ Church Primary 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 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:

- regular meetings with the Computing/Online Safety Leader and Designated Safeguarding Leader
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Curriculum and Standards Committee

Headteacher and Senior Leaders responsibilities:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the Christ Church Primary School community, though the day to day responsibility for online safety will be delegated to the Computing / Online Safety Leader and Governor.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Leader and Governor 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 and Senior Leaders ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- A Senior Leader will specifically be responsible for monitoring the school filtering system via Futures Cloud every week.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Leader.
- The Headteacher and another member of the Senior Leadership Team 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")

  (Misuse is defined by this policy as inappropriate use of school systems which deflects from the learning objectives of the lesson. Some serious incidents of misuse may fall under the school's safeguarding policy and the relevant procedures should then be followed.)

The Online Safety Leader:

- leads the Online Safety Group
- 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 the Local Authority
- receives reports of online safety incidents from a member of the Senior Leadership Team via Futures Cloud monitoring protocols. Logs of incidents are recorded and are used to inform future online safety developments
- meets regularly with Computing/Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant Curriculum and Standards Committee meetings
- reports regularly to Senior Leadership Team. Investigation / action / sanctions will be the responsibility of the Class teacher and or the Senior Management team

The Entrust ICT technician is responsible for ensuring that:

- Christ Church Primary School’s ICT infrastructure is secure and is not open to misuse or malicious attack
- Christ Church Primary School meets the online safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy
- users may only access Christ Church Primary School’s networks through a properly enforced password protection policy, in which passwords are regularly changed
- Entrust Learning Technologies are informed of issues relating to the filtering applied by Netsweeper
- Christ Church Primary School’s filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

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 Christ Church Primary School’s Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Computing/Online Safety Leader / Headteacher for investigation
- digital communications with pupils/parents/carers (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- pupils understand and follow Christ Church Primary School’s Online Safety and Acceptable Use Policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor computing activity in lessons, extra-curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- How to stay safe online posters are displayed in every classroom and that online safety lessons are taught every term according to Christ Church Primary School’s online safety curriculum.

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community including teaching and non-teaching staff, Governors, parents and pupils where appropriate, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives. The group is also responsible for regular reporting to the Governing Board.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Leaders with:

- the production / review / monitoring of the school online safety policy / documents.
- the production / review / monitoring of the school filtering policy.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents/carers and pupils about the online safety provision

Pupils:

- are responsible for using Christ Church Primary School's digital technology systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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 and realise that Christ Church Primary Schools' Online Safety Policy covers their actions out of school, if related to their membership of Christ Church Primary 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of technology than their children. Christ Church Primary School will take every opportunity to help parents understand these issues through newsletters, letters, the school website and information about national local online safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy.
- accessing Christ Church Primary School website and Learning Platform in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – 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 Christ Church Primary 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. Christ Church Primary School will actively make use of the Learning Platform to provide a safe environment for pupils to create blogs, wikis and discussions. Staff will monitor its use and create and encourage good use and discussion etiquette that can be transferred into the wider online community.

Online safety education will be provided in the following ways:

• Online safety should be a focus in all areas of the curriculum and messages should be reinforced across all areas of the Computing curriculum. There will be a planned programme of online safety lessons in the Computing and PSHE curriculum.
• Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities that is targeted appropriately at the relevant key stage.
• Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
• Pupils should be helped to understand the need for the AUP and encouraged to adopt safe and responsible use of computers, the internet and mobile devices both within and outside school.
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
• Pupils are aware of how to respond to inappropriate content and know that a CEOP button is available via the school website for reporting misuse.
• Rules for use of ICT systems / internet safety are posted in all rooms and displayed on log-on screens together with a dedicated display board for online safety
• Acceptable use policies, included in all pupil welcome packs, outline acceptable use of school computers and devices on school property. Parents are asked to read this with their child and sign to agree to the terms before children can access the devices within school. Children in KS1 and KS2 are given relevant policies for their age group.
• Children should be taught about the dangers of the internet and how cyber bullying can occur.
• Children should understand that all incidents of cyberbullying will be dealt with in accordance with Christ Church Primary School's anti-bullying policy.
• Audits are used to assess the views of children and the extent of their online safety issues, allowing a relevant online safety curriculum to be devised.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Review 2008).

Christ Church Primary School therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website and Parent Workshops.

Parents are informed of the CEOP button on the school website and how to deal with reports of misuse.

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 Christ Church Primary School's online safety policy and Acceptable Use Policies.
- Staff will be aware of the procedures to follow if misuse occurs – the use of the CEOP button on the website and the Staffordshire Local Authority "Responding to incidents of misuse" flowchart in the staffroom.
- The Computing Leader will attend regular CPD courses covering changes to acceptable use policies and internet safety.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Computing Leader, with the support of additional external agencies provides advice / guidance / training as required to individuals as required. External agencies include: Educational welfare officers, community police officers and the Safer Internet Day association
- Staff are trained to identify children at risk of being drawn into terrorism and challenge extremist ideas. Enabling them to both recognise the signs of extremism and counter the online extremism.

Training-Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of online safety committee and are involved with child protection. This may be offered by:

- Participation in school training information sessions for staff.

Technical – infrastructure / equipment, filtering and monitoring

Christ Church Primary School is 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 by employing Entrust. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems are managed in ways that ensure that Christ Church Primary School meets the online safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy.
- There are fortnightly reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the Computing Leader and are reviewed annually.
- All users are provided with a username and password by the Computing Leader who keeps an up to date record of users and their usernames. Users are required to change their password every term, unless they are in KS1 when they are expected to change their passwords every year. Staff are also required to change their passwords every term. It is recommended that all users use a mixture of a memorable word and numbers.
- The “master / administrator” passwords for the school ICT system, used by the Computing Leader and SLT are available to the Headteacher and kept in the fire safe.
- Users are responsible for the security of their username and password; they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Christ Church Primary School uses the managed filtering service provided by Netsweeper. Relevant SSL certificates have been installed on all computers and mobile devices to allow the managed filtering service to monitor google searches since the change to the new HTTPS search protocols.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and agreed by the Headteacher
- Any filtering issues should be reported immediately to Entrust Learning Technologies
- A member of the Senior Leadership Team monitors and records weekly the activity of users on Christ Church Primary School’s ICT systems via Futures Cloud and a log of online safety incidents is kept and reported to the Computing/Online Safety Leader. Users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view user’s activity
- An appropriate system is in place for users to report any actual / potential online safety incident to the Network Manager.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of Christ Church Primary School's systems and data.
• An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto Christ Church Primary School system.
• An agreed policy is in place regarding the extent of personal use that users are allowed on laptops and other portable devices that may be used out of school.
• An agreed policy is in place that staff are not allowed to install programmes on school workstations / portable devices.
• An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices
• Christ Church Primary School infrastructure and individual workstations are protected by up to date virus software.
• Personal data must not be sent over the internet or taken off the school premises unless safely encrypted or password protected. CTF files will be used on the school to school secure website to ensure that the transfer of personal information is secure

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with publishing digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Christ Church Primary 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.
• Staff 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 Christ Church Primary School into disrepute
• Pupils must not take, use, share, publish or distribute images of others without their permission. All staff are provided with a list of children who cannot have their photograph taken at school
• 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.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Each class teacher is provided with an up to date list of all children for whom consent has not been given.
- All staff are not to use mobile phones or personal photographic devices in class.

Social Networking

Staff are aware that their conduct on social networking sites cannot:

- Make comments about the school or members of the school community that may bring the school or its members into disrepute
- Make comments about the local authority that may bring the local authority into disrepute
- Post images of the Christ Church Primary School community without their prior consent
- Teaching staff cannot accept friend requests from pupils both past and present.
- It is recommended that teaching staff do not accept friend requests from parents at Christ Church Primary School.

Data Protection

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

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

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 (many memory sticks / cards and other mobile devices cannot be password protected).

- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

.

Communications

When using communication technologies Christ Church Primary School considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored.
• Users need to be aware that email communications may be monitored
• Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
• Any digital communication between staff and pupils or parents / carers (email, chat, Learning Platform etc) must be professional in tone and content and using school provided e-mail addresses.
• Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

If a child in school is involved in inappropriate activity on the school systems, the behaviour policy would be followed. If staff are involved in inappropriate activity inside or outside of school Christ Church Primary School would follow the Staffordshire Local Authority Disciplinary Guidelines.

Responding to incidents of misuse

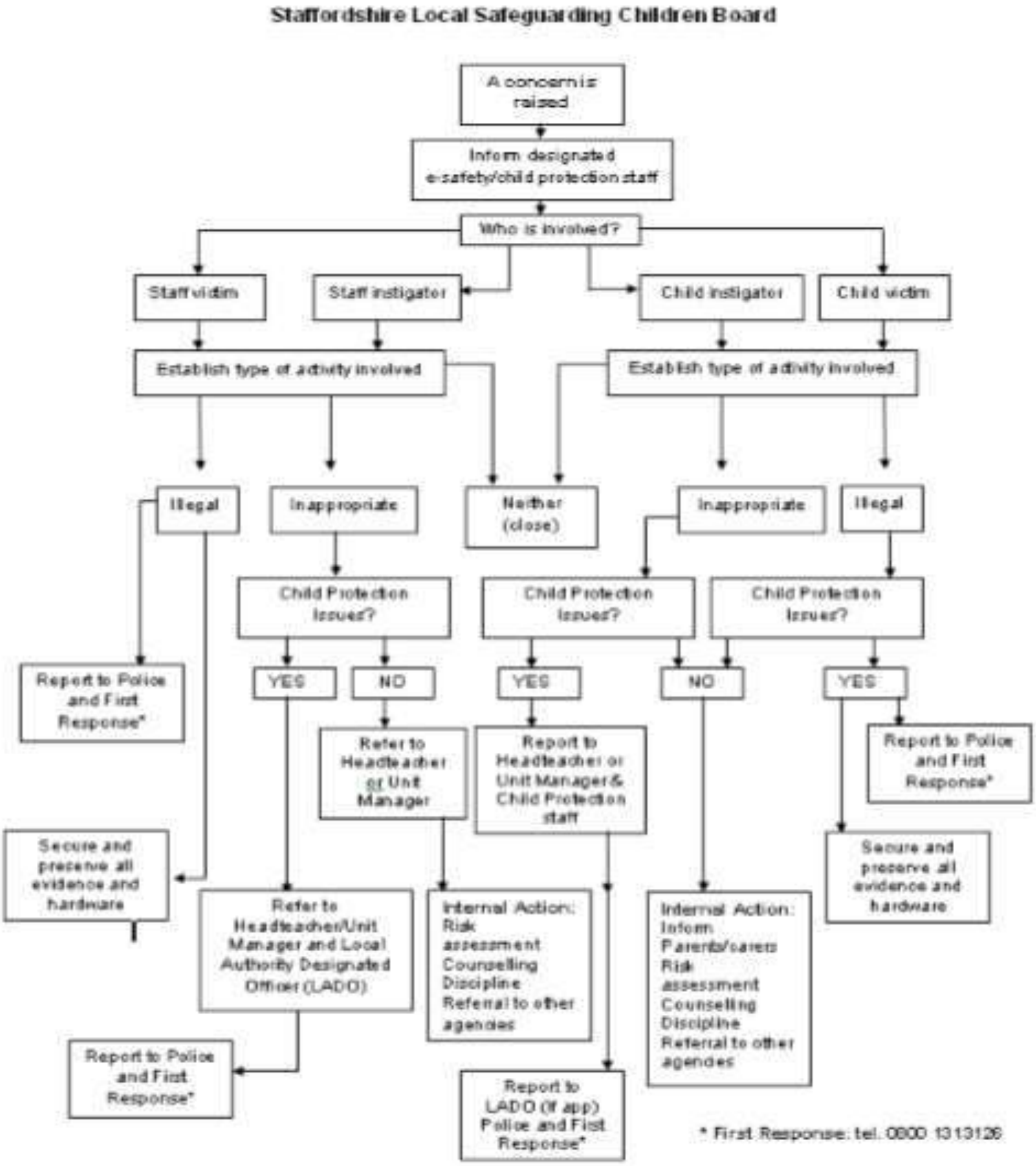
It is hoped that all members of the Christ Church Primary School community will be responsible users of computers, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

• child sexual abuse images
• adult material which potentially breaches the Obscene Publications Act
• criminally racist material

• other criminal conduct, activity or materials.

The Staffordshire flow chart – below and should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



Staffordshire Local Safeguarding Children Board

A concern is raised
Inform designated e-safety/child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police and First Response*
YES
NO
YES
NO
YES
Report to Police and First Response*
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection staff
Secure and preserve all evidence and hardware
Secure and preserve all evidence and hardware
Refer to Headteacher/Unit Manager and Local Authority Designated Officer (LADO)
Internal Action: Risk assessment Counselling Discipline Referral to other agencies
Internal Action: Inform Parents/carers Risk assessment Counselling Discipline Referral to other agencies
Report to Police and First Response*
Report to LADO (if app) Police and First Response*

* First Response: tel. 0800 1313126

The Staffordshire Safeguarding Children Board Online Safety Toolkit found in appendix 1 can also be referred to.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. We recommend that more than one member of staff is involved in the investigation.

It is more likely that Christ Church Primary 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 Christ Church Primary School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures:

Date on which policy was approved: September 2017

Policy reviewed date: September 2018

Next Review: December 2018