Totley All Saints

Church of England Primary School

Online Safety Policy

Enjoy Achieve Learn Succeed Share

Totley All Saints CofE Primary School

TOTLEY ALL SAINTS

Believe Aspire Support Grow Care

Sheffield City Council

"I have come that they may have life,

and have it to the full."

John 10:10

Subject Leader: Julie Brown

Reviewed: Spring 2020
Approved by Governors: Summer 2020
Date of next review: Spring 2022

Online Safety Policy

Policy Introduction

At Totley All Saints, we aim to provide a caring environment where every child can thrive and is supported to achieve their unique & amazing potential as a child of God. As such, this means that…
We believe that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

The school has a duty to provide quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions, and to ensure that children are protected from potential harm online.

The purpose of Online Safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure a safe and secure environment.
- Safeguard and protect all members of the school community online.
- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the school community.

Scope of the Policy

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

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data protection, image use, Acceptable Use Policies (AUPs), confidentiality and relevant curriculum policies including computing, Personal Social Health and Citizenship Education (PSHCE) and Sex and Relationships education (SRE).

Development / Monitoring / Review of this Policy

This policy has been developed by a working group / committee made up of

- Headteacher / Senior Leadership Team
- Online Safety Lead
- Staff – including Teachers
- Parent Governor

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

Schedule for Development / Monitoring / Review

Title	**Totley All Saints Cof E Primary school**
Version	1.0
Date	*March. 2022*
Author	*Online Safety Lead / Team*
Approved by the Governing Body on*:*	
Monitoring will take place at regular intervals:	*Bi-annually*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any Online Safeguarding incidents at regular intervals:	*annually*
The 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 Safeguarding or incidents that have taken place. The next anticipated review date will be:	*Annually*
Should serious Online Safeguarding incidents take place, the following external persons / agencies should be informed:	*DSL/ LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils (including Every Child Matters Survey where applicable)
  - mothers/fathers / carers
  - staff

Communication of the Policy

- The senior leadership team will be responsible for ensuring the school community are aware of the existence and contents of the school online safeguarding policy and the use of any new technology as and when appropriate.
- The online safeguarding policy will be provided to and discussed with all members of staff formally.

- All amendments will be published and appropriately communicated to all members of the school community.
- Any amendments will be discussed by the School / School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An online safeguarding training programme will be established across the school and will include a regular review of the online safeguarding policy.
- Online safeguarding training will be part of the induction programme / transition programme across the Key Stages.
- The Online safeguarding policy will apply when pupils move between education and training providers and will be communicated to all parties accordingly.
- The school approach to online safeguarding and its policy will be reinforced through the curriculum.
- The key messages contained within the online safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed online safeguarding messages across the curriculum whenever the internet or related technologies are used
- The online safeguarding policy will be introduced to the pupils at the start of each academic year
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

We believe that Online Safeguarding is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities technology offers in learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

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 *Safe Guarding Governor*

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Responsibilities of Headteacher and Senior Leaders:

The Headteacher has overall responsibility for safeguarding all members of the school community, though the day to day responsibility for Online Safeguarding will be delegated to the Online Safety Lead

- The Headteacher and senior leadership team are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their Online Safeguarding roles and to train other colleagues when necessary.
- The Headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal Online Safeguarding role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the Online Safety Lead
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious Online Safeguarding incident.

- The Headteacher and senior leadership team receive update reports of any incidents from the Safeguarding team.

Responsibilities of the Online Safeguarding Team

- To ensure that the school Online Safeguarding policy is current and relevant.
- To ensure that the school Online safeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

Responsibilities of the Online Safeguarding Lead

- To promote an awareness and commitment to Online Safeguarding throughout the school.
- To be the first point of contact in school on all Online Safeguarding matters.
- To take day-to-day responsibility for Online Safeguarding within school and to have a leading role in establishing and reviewing the school Online Safeguarding policies and procedures.
- To lead the school Online Safeguarding group
- To have regular contact with other Online Safeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with school technical staff.
- To communicate regularly with the designated the Safeguarding governor.
- To communicate regularly with the senior leadership team.
- To create and maintain Online Safeguarding policies and procedures.
- To develop an understanding of current Online Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online Safeguarding issues.
- To ensure that Online Safeguarding education is embedded across the curriculum.
- To ensure that Online Safeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online Safeguarding issues to the Online Safeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident.
- To ensure that an Online Safeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To understand, contribute to and promote the school's Online Safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the Online Safeguarding lead
- To develop and maintain an awareness of current Online Safeguarding issues and guidance including online exploitation, radicalisation and extremism, bullying, sexting etc.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed Online Safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.

- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of Online Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using only approved and encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To understand, contribute to and help promote the school's Online Safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any Online Safeguarding related issues that come to your attention to the Online Safeguarding lead
- To develop and maintain an awareness of current Online Safeguarding issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the senior management team, local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, Governors, work placement students and volunteers

Communication between adults and between children and adults by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, governors and volunteers should:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child or parent/carers on social networks.

- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children, parent/carers so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children and young people in their care or parents/carers (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the school into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Designated Safeguarding Lead

- To understand the issues surrounding the sharing of personal or sensitive information and to ensure that personal data is protected in accordance with the Data Protection Act 1998.
- To understand the risks and dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving the grooming of children and young people in relation to sexual exploitation, radicalisation and extremism.
- To be aware of and understand online bullying and the use of social media and online gaming for this purpose.

Responsibilities of pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of Online Safeguarding policies and practices and to adhere to those the school creates.
- To know and understand school policies on the use of digital technologies including mobile phones, digital cameras and any other personal devices.
- To know and understand school policies on the use of mobile phones in school.
- To know and understand school policies regarding online bullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the potential risks such as online exploitation, radicalisation, sexting and online bullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss Online Safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting Online Safeguarding.

- To read, understand and promote the school's Online Safeguarding policy and the pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online Safeguarding concerns with their children, be aware of what content, websites and Apps they are using, apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology and social media.
- To consult with the school if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a safe and responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision. Children need the help and support to recognise and mitigate risks and build their resilience online.

Online Safety will be part of a broad and balanced curriculum and staff will reinforce Online Safety messages. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned Online Safety curriculum will be provided as part of PHSE / SRE / Computing and other lessons and should be regularly revisited.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and PHSE activities, including promoting Safer Internet Day each year.
- Pupils will 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 will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- We will discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which they will sign/will be displayed throughout the school
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- 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 SLT can instruct technical staff to temporarily or permanently 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.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Pupils will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies; e.g. mother/father or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

All Staff (including Governors)

It is essential that all staff receive Online Safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- All staff will receive regular information and Online Safeguarding training through a planned programme of PDMs
- All new staff will receive Online Safety information and guidance as part of the induction process, ensuring that they fully understand the Online Safeguarding policy and Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the Online Safeguarding of children and know what to do in the event of misuse of technology by any member of the school community.
- This Online Safeguarding policy and its updates will be presented to and discussed by staff in staff / PDMs / INSET days.
- An audit of the Online Safety training needs of all staff will be carried out regularly.
- The Online Safety Lead will provide advice, guidance and training as required.

Parents/Carers

Mothers / Fathers / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and responsible way and in promoting the positive use of the internet and social media. Many have only a limited understanding of Online Safety risks and issues, yet it is essential they are involved in the Online Safety education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may under-estimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for the Safeguarding Governor. This may be offered in a number of ways:

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

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential risks associated with sharing images and with posting 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. The school will inform and educate users about these risks and their legal responsibilities and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff will inform and educate pupils about the risks and current law associated with the taking, sharing, use, publication and distribution of images. In particular they should recognise the risks attached to publishing inappropriate images on the internet or distributing through mobile technology.

- Staff are allowed to take digital / video images to support educational aims or promote celebrations and achievements, 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, including mobile phones, 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. Staff will be aware of those pupils where publication of their image may put them at risk.

- Pupils' full names will not be used in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

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

- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Managing ICT systems and access: Technical infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the 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 identified in the previous section will be effective in carrying out their Online Safeguarding responsibilities.

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible and meets recommended technical requirements.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- The infrastructure and appropriate hardware are protected by active, up to date virus software.
- There will be regular reviews and audits of the safety and security of technical systems.
- IT 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
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

- Servers, workstations and other hardware and software will be kept updated as appropriate.
- The "administrator" passwords for the school ICT system, used by the IT Manager (or other person) must also be available to the Headteacher and kept in a secure place (eg safe)
- All users will have clearly defined access rights to school technical systems and devices.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- At Y4, 5, 6 pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the staff AUP at all times.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to (online safeguarding team as agreed.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Filtering internet access

'Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.'

- The school uses a filtered internet service. The filtering system is provided by Smoothwall
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed, sent or received through the school's internet provision.
- The school will ensure that the filtering system will block extremist content and protect against radicalisation in compliance with the Prevent Duty, Counter-Terrorism and Security Act 2015
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Lead. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead.
- The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and Government Prevent block list and this will be kept updated..
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1 pupils and Y3 will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Y4 and above will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems.
- All information systems require end users to change their password at first log on.
- Users will be prompted to change their passwords regularly or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users 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.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer-based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords should comply with current accepted complexity recommendations.

Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to 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	✓							✓

Unsuitable / Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 Radicalisation or extremism in relation to the Counter Terrorism and Security Act 2015					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing		X				
Use of social media		X				
Use of messaging apps		X				
Use of video broadcasting eg Youtube		X				

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, 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 e.g.

- child sexual abuse images

- adult material which potentially breaches the Obscene Publications Act
- criminally racist material, radicalisation and extremism
- other criminal conduct, activity or materials

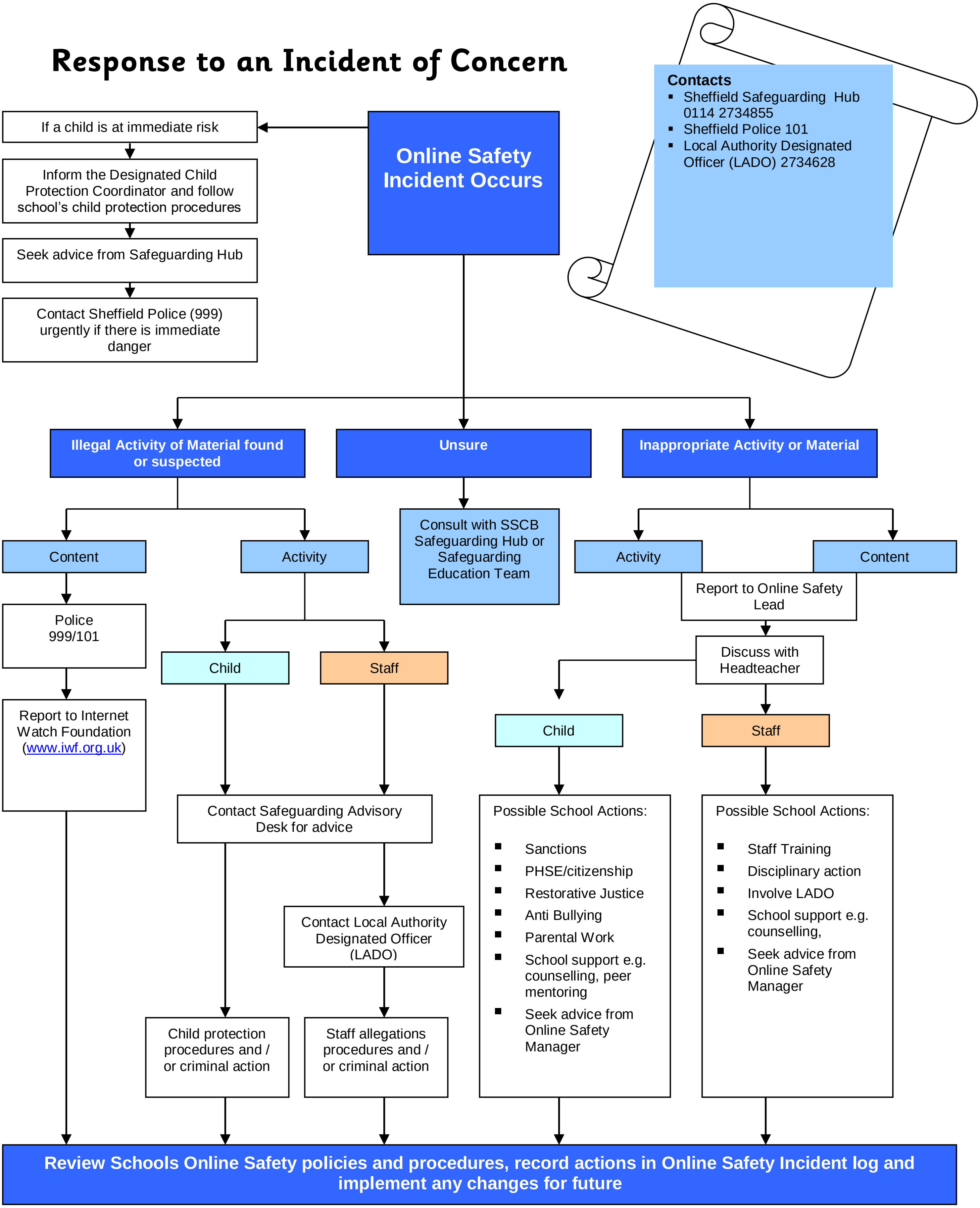
The SSCB flow chart should be consulted and actions followed in line with the flow chart.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

Dealing with Online Complaints

- Parents/Carers are reminded through the Home-School Agreement of appropriate complaints channels and procedures.
- The complaint policy/procedure is clearly detailed on the school website and within the Complaints policy
- All staff and governors are aware of how to report any negative online comments about the school or members of the school community.
- Staff and governors must under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the Headteacher.

Response to an Incident of Concern



Contacts

- Sheffield Safeguarding Hub 0114 2734855
- Sheffield Police 101
- Local Authority Designated Officer (LADO) 2734628

Online Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Hub

Contact Sheffield Police (999) urgently if there is immediate danger

Illegal Activity of Material found or suspected

Content

Police 999/101

Report to Internet Watch Foundation (www.iwf.org.uk)

Activity

Child

Staff

Contact Safeguarding Advisory Desk for advice

Contact Local Authority Designated Officer (LADO)

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Unsure

Consult with SSCB Safeguarding Hub or Safeguarding Education Team

Inappropriate Activity or Material

Activity

Content

Report to Online Safety Lead

Discuss with Headteacher

Child

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Seek advice from Online Safety Manager

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- Involve LADO
- School support e.g. counselling,
- Seek advice from Online Safety Manager

Review Schools Online Safety policies and procedures, record actions in Online Safety Incident log and implement any changes for future

Contact Details

Schools Designated Child Protection Officer: Karole Sargent
School Online Safety Coordinator: Julie Brown

Appendices

.

- Further Information
- Use of Digital Images
- Links to other organisations, documents and resources
- Legislation

Further Information

- Training is available via Safeguarding Training Service on 0114 Telephone: 0114 2735430 or email safeguardingchildrentraining@sheffield.gov.uk

- The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around Online Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.

- "Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety

- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx

- 360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk/

- "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidanc

Use of Photographs, videos and other images within School

This applies to all staff, volunteers and students on work placement.

There are a number of things that you need to address when using images of people, especially children, some of which is contained in the Data Protection Act 1998:

- You must get the consent of all parents of children appearing in the photograph or video/DVD image before it is created
- You must be clear why and what you'll be using the image for and who will see it
- If you use images from another agency, you need to check that the agency has obtained informed consent

Safeguarding issues:

- Use equipment provided by the school to take the images and not personal devices
- Download and store images in a password protected area of the school network not on personal computers
- When images are stored on the system they should be erased immediately from their initial storage location e.g. camera
- Don't use full names or personal contact details of the subject of any image you use
- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner
- No images of a looked after child should be created or used without prior consent from Children's Social Care
- Don't use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use
- Always destroy images once consent has expired or the child has left your school

Consider:

- Are CCTV (security) cameras sited where they may compromise the privacy of individuals?
- How public are your display boards?
- What is the purpose and audience of video's and DVD's you have created?
- Are all of your images and media securely stored at your school?
- Images on websites, and other publicity can become public and outside your control
- Any implications of using images offsite
- The press are exempt from the Data Protection Act, if you invite them to your premises or event, you need to obtain prior consent from parents of children involved
- Including images from different ethnic groups and those of disabled children
- Check out any copyright implications

The Information Commissioner's Office guidance advises that photographs taken for personal use e.g. by parents at special events, at an education setting are not covered by the Data Protection Act.

Useful links/resources:

- ○ **The Use of Cameras and Images within Educational Settings and in Social Media**
- ○ **Online Safety section** **www.safeguardingsheffieldchildren.org.uk**
- ○ **Photographs and Videos, Information Commissioners Office, at:** http://www.ico.gov.uk/for_the_public/topic_specific_guides/schools/photos.aspx

Links to other Organisations or Documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Sheffield Safeguarding Children Board http://www.safeguardingsheffieldchildren.org.uk

Safer Internet Centre: http://www.saferinternet.org.uk/

UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis

CEOP - Think U Know - http://www.thinkuknow.co.uk/

Childnet - http://www.childnet.com

Netsmartz http://www.netsmartz.org/index.aspx

Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/

Guidance for safer working practice for adults that work with children and young people - http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/

Information Commissioners Office/education and ICO guidance on use of photos in schools: www.ico.org.uk

Plymouth Early Years Online Safety Toolkit:
http://www.plymouth.gov.uk/early_years_toolkit.pdf
Protecting your personal information online: http://www.ico.org.uk
Getnetwise privacy guidance: http://privacy.getnetwise.org/

Children and Parents

Safer Internet Centre: http://www.saferinternet.org.uk/
CEOP - Think U Know - http://www.thinkuknow.co.uk/
Vodafone Parents Guide: http://parents.vodafone.com/
NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone: www.parentinfo.org
Childnet - http://www.childnet.com
Internet Matters: www.internetmatters.org
CBBC – stay safe: http://www.bbc.co.uk/cbbc/

Technology

CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/
Internet Matters: www.internetmatters.org
Get Safe Online: www.getsafeonline.org

Microsoft Family safety software: http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety

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.

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.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

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 Harrassment 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 priso

Sexual Offences Act 2003

The new 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 the 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. The 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 / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Counter-Terrorism and Security Act 2015

From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".

The statutory guidance on the Prevent duty summarises the requirements on schools and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies.

SSCB would like to acknowledge YHGfL, SWGfL and Kent County Council for the use of their documentation.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of review and update October 2017. However, SSCB cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.