Crucible Federation

Whiteways and Owler Brook Primary Schools

Online Safeguarding Policy

Policy Introduction

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 of school.

The internet and other digital and information technologies are powerful tools, which can 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 should 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. A school online safety policy should help to ensure safe and appropriate use by all users.

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 the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Loss of privacy / control of personal information
- Grooming or exploitation by people who they make contact with on the internet.
- The sharing / distribution of personal images and personal information without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying
- Access to unsuitable video / internet games
- Being unable to judge the accuracy, relevance and reliability of information
- Plagiarism (copying a piece of written work or an idea and claiming it as your own) and breach of copyright (the illegal copying or use of creative work e.g. music, video, photographs, documents etc. without the owner's consent)
- Illegal downloading of music or video files
- Hacking into personal profiles, ineffective system security and viruses (giving access to personal and financial information)
- The potential for excessive use which may impact on the social and emotional development and learning of the child or young person.

Many of these risks reflect situations in the off-line world and this online safety policy is used in conjunction with other school policies such as behaviour, anti-bullying, data protection, use of social media, child protection, teaching and learning (computing and PHSE) policies.

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build resilience to the risks to which pupils may be exposed, so that they have the confidence and skills to face and deal with these risks.

The 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, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

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

- **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. This applies to incidents of cyber-bullying, or other Online Safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- **The Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others. https://www.gov.uk/government/publications/searching-screening-and-confiscation

- The school/college will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform mothers / fathers / carers of incidents of inappropriate Online Safeguarding behaviour that takes place out of school / college. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.

- **Keeping Children Safe In Education September 2018** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what schools and colleges **should** do and sets out the legal duties with which schools and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2018**

- **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.

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Development /Monitoring/Review of this Policy

The Crucible Federation has an online safety team made up of members of the safeguarding team, Heads of School, School Business Manager and Network Manager. Our online safety policy has been written by both schools, in line with Sheffield Safeguarding Children's Board policies and Keeping Safe in Education 2018. It has been agreed by the senior management team and approved by governors.

The online safety policy will be reviewed annually. This policy will next be reviewed in September 2019.

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

Schedule for Development / Monitoring / Review

Title	**Crucible Federation Online Safeguarding Policy**
Version	2.0
Date	September 2018
Author	Lisa Whitehead and Claire Shaw
Approved by the Governing Body on*:*	
Monitoring will take place at regular intervals:	Termly
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 (termly update of incidents at governors meetings)
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:	September 2019
Should serious Online Safeguarding incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office, Safeguarding Sheffield Children's Board

The schools will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / 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 schools 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 online safety team and 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 for new staff.
- The online safeguarding policy will apply when pupils/students move between education and training providers eg on educational visits and will be communicated to all parties accordingly.
- The school approach to online safeguarding and its policy will be reinforced through the curriculum / programme of study.
- 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/students 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 Online Safety Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator/team
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering/change control logs

- reporting at relevant governors meetings

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/team.

- 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 (see flow chart on dealing with Online Safety incidents) and relevant disciplinary procedures.
- The Headteacher and senior leadership team receive update reports of any incidents from the Online Safeguarding/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 Coordinator

- 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 or committee.
- 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 Online 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 (including supply 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 coordinator.
- 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 coordinator.
- 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/young people 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/young person, 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/young person 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 (GPDR after May 2018).
- 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 Students / 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.

To sign a home-school agreement containing the following statements

- *We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community*
- *We will support the school's Online Safeguarding Policy.*
- *Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet*
- *Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.*
- *Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school*
- *Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.*

Responsibilities of Other Community/External Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

- Any external users/organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision, filtering and monitoring exist when external users/organisations make use of the internet and ICT equipment within 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 and young people 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 Computing/PHSE/SRE and other lessons and will be regularly revisited.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and class 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 and will be displayed when a user logs on to the network.
- 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, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the designated safeguarding lead and/or deputy designated safeguarding lead 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 staff meetings and updates.
- 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 meetings.
- An audit of the Online Safety training needs of all staff will be carried out regularly.
- The Online Safety Coordinator/ 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 and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, web site
- Parents' 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 those who are involved in Online Safety and child protection. 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).

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide Online Safety information for the wider community

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.

(See SSCB document 'The Use of Cameras and Images within Educational Settings and on Social Media')

- 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 has a managed ICT service provided by an outside contractor (CBC). Our schools are responsible for ensuring that the managed service provider carries out all the appropriate Online Safety measures and complies with the schools Online Safeguarding Policy and Acceptable Use Agreements.

The schools will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will also 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.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations 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 Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. 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.
- In Y5 and Y6, pupils will have an individual user account provided by the Network Manager 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 the Designated Safeguarding Lead and/or Head of School as agreed.
- An appropriate system is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An appropriate system is in place regarding the extent of personal use that users (staff/ pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An appropriate system is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An appropriate system 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

Teachers may decide to request that certain websites are allowed temporarily for specific users. Teachers should be able to justify why they may decide to change the filtering systems, to record such a change and ensure that they have sufficient procedures and audit trails in place to deal with an Online Safeguarding incident arising from a level of filtering which differs from normal. Requests for a website to be unblocked need to be made to the Network Manager using the reporting system Every. The Network Manager then liaises with the school DSL and/or Head of School for permission to unblock the website. This is then logged as part of the audit trail.

In addition to a filtering solution, the schools have installed a monitoring system that analyses activity on computers and flags up possible inappropriate use and language as an additional security measure. The monitoring software being used is Netsweeper.

A recognised incident-management procedure is in place to ensure that any incidents relating to unsuitable internet content being viewed within school is dealt with appropriately. All staff and pupils are aware of how to report/record incidents which should then be reviewed so that appropriate controls, measures or awareness sessions can be put in place.

- The school uses a filtered internet service. The filtering system is provided by Netsweeper.
- 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

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly-chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen or a school/college network being infected or attacked.

The school has a responsibility to ensure that all elements of the school infrastructure and network equipment are as safe and secure as possible. All staff and pupil access to school-owned equipment and information assets should be controlled through the use of appropriate username and password policies.

It is important that all pupils and staff have an awareness of how to construct a complex and secure password as well as understanding the security implications of not protecting the password once selected. It is generally accepted that pupils at and above upper Key Stage 2 should have an individual account for accessing ICT systems within school. Key Stage 1 pupils could have generic 'pupil' accounts with standard passwords.

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1 and lower Key Stage 2 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at upper Key Stage 2 and above 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 every 60 days (on CPOMS) 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.

General Data Protection Regulation (GDPR)

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

For information on how we collect, store and process data collected please refer to our Data Protection Policy and Privacy Policies.

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		✓					✓	

*School Google Mail Instant Messaging only

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

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- 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 agreed channel of digital communication between staff and pupils or parents/carers must be professional in tone and content.

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					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	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					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	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				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	

Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				✓	
On-line gaming (educational)		✓	✓		
On-line gaming (non educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing				✓	
Use of social media				✓	
Use of messaging apps		✓	✓		
Use of video broadcasting eg Youtube		✓	✓		

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 suspects 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

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓	✓	✓	✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓							✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓							✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓		✓	
Unauthorised downloading or uploading of files		✓	✓			✓		✓	✓
Allowing others to access school network by sharing username and passwords	✓	✓			✓			✓	
Attempting to access or accessing the school network, using another student's / pupil's account	✓	✓			✓			✓	✓
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓		✓	✓		✓	✓
Corrupting or destroying the data of other users	✓	✓			✓	✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓	✓	✓		✓	✓
Continued infringements of the above, following previous warnings or sanctions			✓		✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓		✓	✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system			✓		✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material			✓		✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓			✓	✓		✓	

In the worst case scenario: The head will investigate any inappropriate use of digital technology and seek advice from safeguarding services and other agencies where appropriate.

Staff Actions / Sanctions

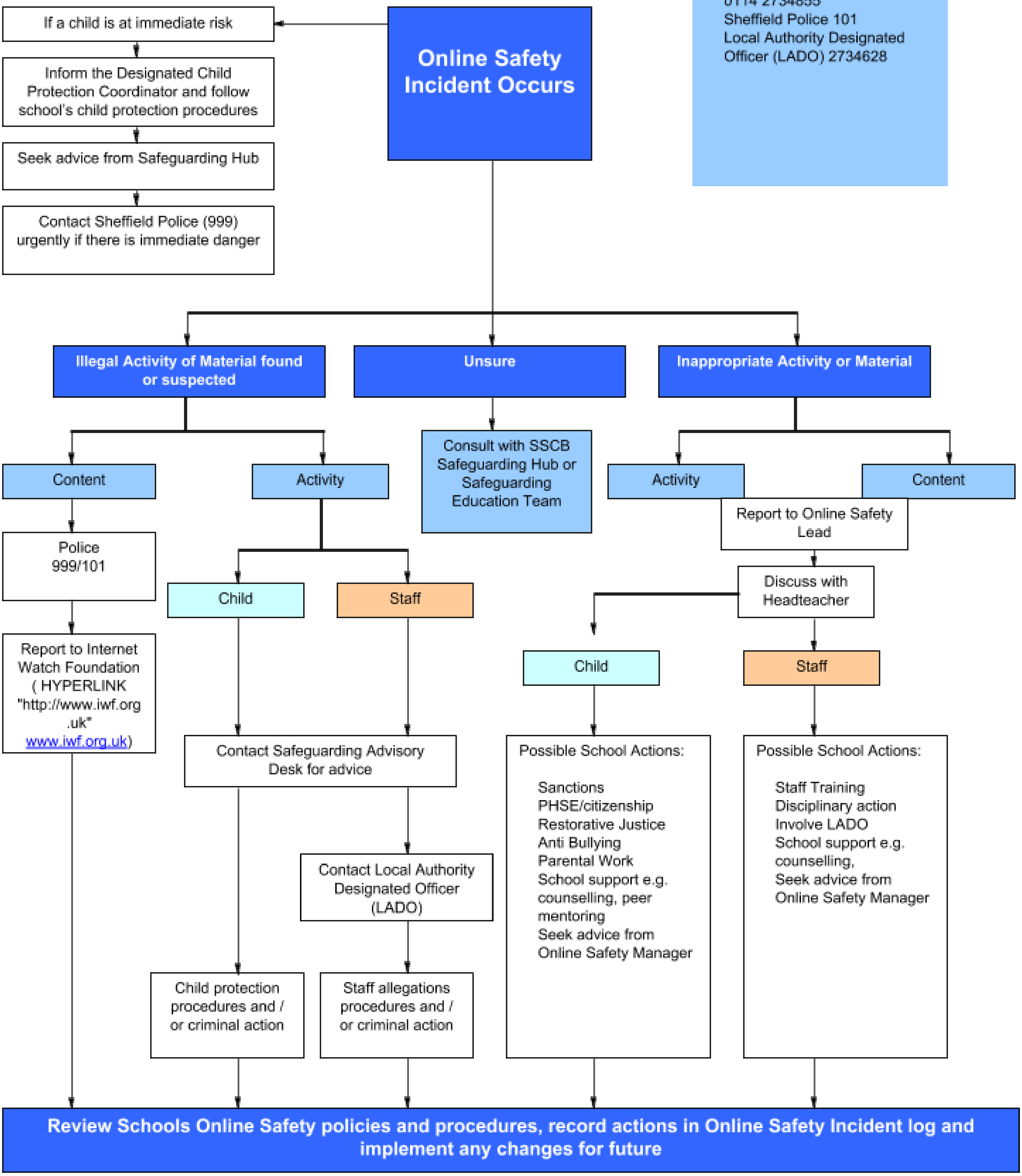
Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓		✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓			✓	✓		
Unauthorised downloading or uploading of files		✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓			✓	✓		
Careless use of personal data eg holding or transferring data in an insecure manner		✓			✓			✓
Deliberate actions to breach data protection or network security rules		✓			✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓		✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓	✓	✓				✓
Actions which could compromise the staff member's professional standing		✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓						✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓				✓		
Deliberately accessing or trying to access offensive or pornographic material		✓					✓	✓
Breaching copyright or licensing regulations		✓				✓		

Continued infringements of the above, following previous warnings or sanctions		✓						✓

In the worst case scenario: The head will investigate any inappropriate use of digital technology and seek advice from safeguarding services and other agencies where appropriate.

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

Unsure

Inappropriate Activity or Material

Content

Police 999/101

Report to Internet Watch Foundation (HYPERLINK "http://www.iwf.org.uk" 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

Consult with SSCB Safeguarding Hub or Safeguarding Education Team

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

Appendices

- Pupil Acceptable Usage Policy template
- Staff and Volunteers Acceptable Usage Policy template
- Parents/Carers Acceptable Usage Policy Agreement template
- Use of Digital Images and sample Consent Form
- Mobile Phone Use
- Questions for Schools to consider
- Links to other organisations, documents and resources
- Legislation

Acceptable Use Policy for KS1

You can use the school's ICT equipment to access the Internet and to help you with your learning. These rules will help make sure the school network is a safe place for everyone. You will need to agree to follow these rules whenever you use ICT equipment in school.

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer.
- I will only use activities that I have been told to use.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):………………………………… Class:……………….

Key Stage 2 Acceptable Use Policy (AUP)

You can use the school's ICT equipment to access the Internet and to help you with your learning. These rules will help make sure the school network is a safe place for everyone. You will need to agree to follow these rules whenever you use ICT equipment in school.

Using the school ICT equipment:

- I will only use the computers and other devices for school work.
- I will ask permission from a member of staff before using the Internet.
- I will only visit websites to help me with schoolwork that my teacher has said I can go on.
- When I am using the internet to find information, I will take care to check that the information that I find is accurate, as I understand that other people's work may not be correct.
- I will only send messages to people I know, or my teacher has agreed to.
- The messages I send and the work I do will be polite and responsible, and not contain anything that might upset someone else including images.
- I will only open attachments in messages I receive, or download a file if I trust the person who sent it or the website it is from, and I've checked with my teacher that it is safe.
- I will keep my username and password safe by not telling anyone else.
- I will only look at other people's files or messages with their permission.
- I will not give away any of my personal information, or the personal information of people I know, over the Internet. This includes my full name, address, phone numbers, photographs and videos of me and my friends, or the name of my school.
- I will not install, or try to install, any programmes nor will I try to change any settings.
- I understand that the school may check my computer files, the Internet sites I visit, the messages I send and anything else I do to make sure I am keeping myself and others safe

Staying safe:

- I will never arrange to meet anyone that I have never met in real-life before, unless my parent or teacher has given me permission and I take a responsible adult with me.
- If I see or receive anything that is unpleasant, or makes me feel uncomfortable or upset, I will report it to a member of staff immediately.
- If something happens whilst using a computer or school device, and I am not sure what I should do next, I will ask a member of staff to help me.
- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. For example cyber bullying, sending/receiving inappropriate images and misuse of personal information.

Finally, I understand that if I do not follow these rules and other guidance from the school as best as I can then I may not be allowed to use any of the school's ICT equipment.

Signed :……………………………………… Class: …………………..

Staff Acceptable Use Policy (AUP)

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using ICT equipment. All users should follow the guidelines at all times. Staff are responsible for their behaviour and actions when using ICT equipment (including the Internet) at school as well as when they are using portable devices (e.g. laptops and iPads) at other locations (such as their home).

User Responsibilities

- Any use of school ICT equipment, including portable devices, is to be for professional purposes as agreed by the school's senior leadership team.
- Any images/videos of pupils or staff should be for professional purposes only and have the relevant consent. They should be taken on school equipment, and stored and used onsite. Such images should not be taken off-site without permission and valid reason.
- All material on portable devices must be for professional purposes only. Sending, accessing, uploading, downloading or distributing offensive, threatening, pornographic, obscene, illegal or sexually explicit materials is not allowed and will result in disciplinary actions. If you accidentally encounter such material you should follow your school's procedure and report this to the Head of School / Deputy Headteacher / Network Manager immediately.
- Posting of images/videos on the internet into a public forum is strictly forbidden, without the express permission of the Head of School.
- Any online activity should not harass, harm, offend or insult other users.
- Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity is forbidden.
- Users are not allowed to have music or install software (including apps) onto portable devices. However, if a user wishes content to be added to a device, they can request this to be done by the school's Network Manager.
- Users are not allowed to download or install any hardware or software onto the school network without permission. Those responsible for installing software should be confident it is adequately licensed, appropriate for educational use and GDPR compliant.
- Jail breaking (i.e. the process of which removes any limitations placed on by the manufacturer) is strictly prohibited as it results in a less secure device.
- Individual users are responsible for the setting up and use of any home internet connections with portable devices.
- Portable devices are subject to routine monitoring by The Crucible Federation (Owler Brook and Whiteways Schools). Devices must be surrendered immediately upon request by the Head of School / Deputy Headteacher / Network Manager.
- The Crucible Federation is not responsible for the financial or other loss of any personal files that may be deleted from a portable device.

- Personal mobile phones must not be used during the school day other than in staff only areas where they cannot be seen by children, e.g. staffroom. Personal mobiles must not be visible to any child in school at any time, regardless of whether or not they are in use.

Safeguarding and Maintaining as a Tool

- Users must use the protective covers/cases provided for any portable devices.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean a laptop screen.
- Do not subject any portable device to extreme heat or cold.
- Do not store or leave any ICT equipment unattended in vehicles.
- The whereabouts of the laptop should be known at all times.
- It is a user's responsibility to keep the laptop safe and secure.
- If a portable device is lost, stolen, or damaged, the Head of School / Deputy Headteacher / Network Manager must be notified immediately.
- Users must set a password/code on their portable devices to prevent misuse.
- Usernames, passwords/codes and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using ICT equipment. You should not allow an unauthorised person to access the school ICT equipment.
- Items deleted from portable devices cannot be recovered.
- Memory space is limited and work related content takes precedence over personal files on all portable devices.
- Any ICT equipment found unattended should be given to the Head of School / Deputy Headteacher / Network Manager immediately.
- Ensure that any files on removable media (e.g. USB drives and CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Head of School.
- Personal or sensitive information should only be taken off-site if agreed with the Head of School, and must be stored on an encrypted USB device provided by school.
- You should ensure that any personal or sensitive information you use or access (e.g. SIMs data) is kept secure and used appropriately.
- Users are not to have current pupils as friends on social network sites and also need to be aware of the impact other contacts may have. Users must ensure privacy settings are such that only friends may see their profile. Staff should be aware that anything published online which could be viewed by others, (e.g. Facebook or Twitter) and brings the school into disrepute could result in disciplinary action.
- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring the user's professional role or the name of the school into disrepute.

- Users will not give out personal details, or the personal details of other users, to pupils or parents or on the internet. In particular they should ensure their home address, personal telephone numbers and email accounts are not shared with children, young people or parents.
- Users should respect intellectual property and ownership of online resources they use in their professional context, and acknowledge such sources if used.

Finally

- The Crucible Federation reserves the right at any time to confiscate and search ICT equipment.
- Users understand that all files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others.
- The school reserves the right to make appropriate charges if staff persistently fail to keep equipment secure resulting in loss or damage. Such action will be considered on a case by case basis at the discretion of the Head of School.
- The school may decide not to replace equipment which is lost or damaged. Items which are considered to be 'luxury', non-essential items will not be replaced.
- Users in breach of this policy may be subject to but not limited to: disciplinary action; confiscation; removal of content; or referral to external agencies in the event of illegal activity.

I have read and understood the information given to staff on GDPR.

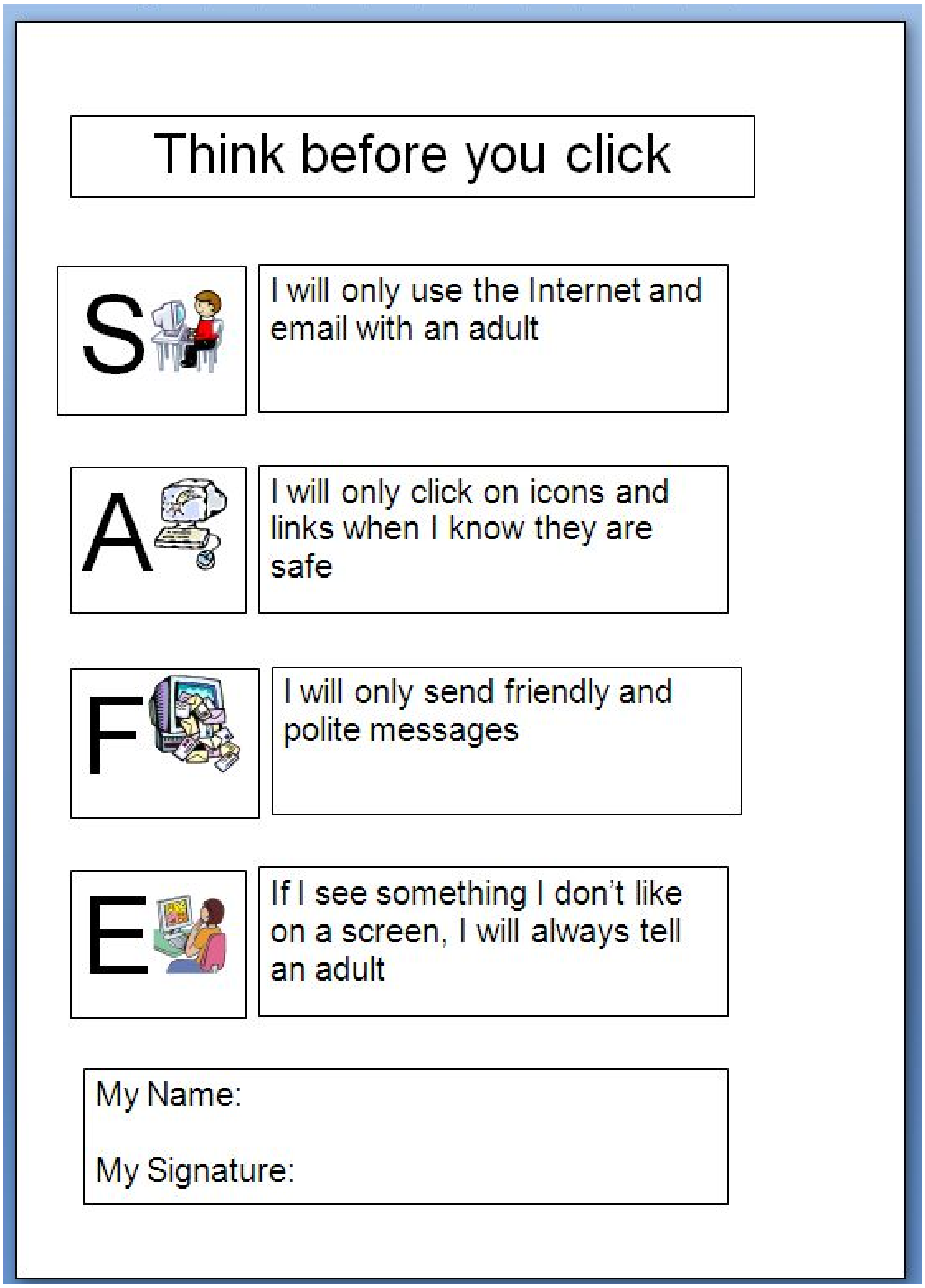
I understand my responsibilities to ensure compliance to the GDPR

Signed ………………………………………………………….

Print name …………………………………………………..

Date …………………………………………………………….

Think Before You Click



Think before you click

S	I will only use the Internet and email with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don’t like on a screen, I will always tell an adult

My Name:

My Signature:

Further Information

- Training is available via Safeguarding Training Service on 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/Guidance%20.pdf

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.

General Data Protection Regulation

This protects the rights and privacy of individual's personal data. for more information on this regulation please refer to the To comply with the ICO website a Guide to GDPR.

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 prison

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 September 2018. However, SSCB cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.