Oughtibridge Primary School

Online Safeguarding Policy

Policy Introduction

This policy outlines our approach to Online Safeguarding in regards to the role of digital technologies in teaching and learning, the benefits and opportunities they bring, and the importance of understanding potential risks.

The use of PCs, laptops, iPads, kindles, digital cameras, programmable devices and any other digital devices, has been considered in the development of this policy. The school ensures that it takes the necessary steps to manage and reduce the risks associated with using digital technology.

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, 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 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 will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents / carers of incidents of inappropriate Online Safeguarding behaviour that takes place out of school. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.
- **Keeping Children Safe In Education September** 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 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 **should** do and sets out the legal duties with which schools **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2015**
- **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

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

- Senior Leadership Team
- Online Safety Lead
- Computing Coordinator
- GDPR Lead

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

Schedule for Development / Monitoring / Review

Title:	Oughtibridge Primary School Online Safeguarding Policy
Version:	2.0
Date:	21/03/2022
Author:	Online Safety Team
	Catherine Askham (GDPR) Stephanie Dennis (Computing and Online Safety Coordinator) Gemma Shelton (SLT – DSL)

Approved by the Governing Body on*:*	
Monitoring will take place at regular intervals:	Once a term
The Governing Body will receive a report on the implementation of the policy including anonymous details of any Online Safeguarding incidents at regular intervals:	Once a term
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:	July 2023
Should serious Online Safeguarding incidents take place, the following external persons / agencies should be informed:	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)
    - parents/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.

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 staff and volunteers.

The school approach to online safeguarding and its policy will be reinforced through the curriculum / programme of study, and explicitly taught at least once a year. We endeavour to embed online safeguarding messages across the curriculum whenever the internet or related technologies are used.

The key messages contained within the online safeguarding policy will be reflected and consistent within all acceptable use policies in place within school and 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
- regular monitoring of Online Safety incident logs

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 Co-ordinator.

- The Headteacher and senior leadership team are responsible for ensuring that the Online Safety Co-ordinator 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 Co-ordinator.
- 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 included on page 23).
- 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 contact with other Online Safeguarding committees (e.g. Safeguarding Children Board) when necessary.
- To communicate as necessary with school technical staff.
- To communicate annually 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

- 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 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, tablets and game consoles.
- 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 their 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 their 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 and volunteers

The following applies to any adult, but particularly those working with children and young people (paid or unpaid) within the school. Consideration should be given to how the online behaviour of staff may affect their own safety and reputation and that of the school.

Communication between adults and communication 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, blogs and online gaming.

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 e.g 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 on social networks.
- only send or accept a friend request from parent/carers on social networks where there is a personal connection.
- 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, incorporating the use of digital technologies (including mobile phones in school) and in regards to 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 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 to read and promote 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 be aware of the school's policy in regards to the taking of photographic images and videos and their use outside of school.
    - *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*
    - *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.*
- To give written consent for the use of any images of their children in a variety of different circumstances (see page 30).

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 the PSHE curriculum (with elements taught through the Computing curriculum) and should be regularly revisited.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral 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 Acceptable Use Policy (see page 24&25) which will be displayed throughout the school 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, 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 Computing Co-ordinator) 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. parents 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 / annual updates etc.)
- 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 / team meetings / INSET days.
- An audit of the Online Safety training needs of all staff will be carried out regularly.
- The Online Safety Coordinator will provide or arrange advice, guidance and training as required.

Parents/Carers

Parents/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:

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

Training – Governors

The Online Safety Governor should take part in training / awareness sessions. 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 local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Online Safety
- 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.

- 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 use of staff's personal equipment, such as mobile phones, should only be used for sending digital images / video during exceptional circumstances (day trips / residentials). Images / video will be deleted from personal devices immediately after being transferred to the school network.
- 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.

Remote learning

- Keeping pupils, students and teachers safe during remote education is essential.
- Remote education could be pre-recorded lessons, virtual lessons, and/or live streaming. Teachers delivering remote education online should be aware that the same principles set out in the school Staff Code of Conduct, Acceptable Use Policy and the rest of this Online Safeguarding Policy will apply.
- All staff, pupils and families using video communication must:
    - Wear suitable clothing – this includes others in their household.
    - Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
    - Use appropriate language – this includes others in their household.
    - Maintain the standard of behaviour expected in school.
    - Use the necessary equipment and computer programs as intended.
    - Not record, store, or distribute video material without permission.
- The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

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

The school 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. 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.
- Bluebox 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 “master / administrator” passwords for the school’s ICT system, used by the Network Manager (or other person) 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.
- By the end of Key Stage 2, pupils will have an individual user account provided by Bluebox 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 (verbally report) for users to report any actual / potential technical incident / security breach to (computing coordinator), as agreed.
- A ‘supply’ login is in place for the provision of temporary access of “guests” (e.g trainee teachers, supply teachers, visitors) onto the school systems.
- Staff are not allowed to use school devices, in or out of school, for personal use
- An agreed policy is in place (see AUP) that forbids staff from downloading executable files and installing programmes on school devices, unless agreed by the computing coordinator (.e.g iPad apps).
- An agreed policy is in place regarding the use of removable media (e.g 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 (see Data Protection and Security Section for further details).

Filtering internet access

- 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 Coordinator. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Coordinator.
- 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 will have a generic 'pupil' logon to all school ICT equipment.
- By the end of Key Stage 2, pupils 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 every half term 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.

Data Protection

Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) (2018) which states that personal data must be:

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

The School will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the DPO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the DPO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the DPO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

When transmitting sensitive information or personal data e.g. by email it must be transferred by a secure method so it is protected from unauthorised access.

Email

- It is advisable not to use public email accounts for sending and receiving sensitive or personal data.
- When sending personal data via email is necessary, personal or sensitive information should not be included within the email itself, as the information sent should be sent by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email. Recipients of the email should be previously aware of the necessary password.
- If appropriate, names within the email should be substituted for initials.

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 with parental permission	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x				x		
Use of mobile phones in lessons			x				x
Use of mobile phones in social time	x						x
Taking photos on mobile phones/cameras		x					x
Use of other mobile devices e.g. tablets, gaming devices		x					x
Use of smart watches		x				x	
Use of personal email addresses in school, or on school wifi network		x					x
Use of school email for personal emails				x			x
Use of messaging Apps		x					x
Use of social media		x					x
Use of blogs	x					x	
Use of technologies for the purpose of remote learning	x				x		

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 and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- 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.

Mobile phone usage in schools

Staff (inc volunteers) use of mobile phones and personal devices

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of SLT.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

Pupil use of mobile phones and personal devices

- Pupils must have signed parental permission to bring a mobile phone to school.
- All mobile phones handed in to the school office on arrival, where they will be stored for the duration of the school day.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Parent use of mobile phones and personal devices when on site

- Mobile phones and other personal devices should not be used whilst on school grounds unless for specifically agreed reasons.

Visitors to the school

When signing in, visitors will be asked to read and agree to the following conditions which is displayed on the signing in book:

“By signing in you agree to the appropriate use of the Internet and any digital devices, in line with our Online Safeguarding policy.”

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					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g 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	
Online gaming (educational)		X				
Online gaming (non educational)			X			
Online gambling					X	
Online shopping / commerce				X		
File sharing (for educational purposes)		X				
Use of social media				X		
Use of messaging apps			X	X		
Use of video broadcasting e.g uploading content to 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 (see page 23) 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

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to SLT	Refer to Headteacher	Refer to Police / ICO	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Sanctions in line with behaviour policy	Further sanctions e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	x	x	x	x	x	x	x	x	x
Unauthorised use of non-educational sites during lessons	x					x		x	
Unauthorised use of mobile phone / digital camera / other handheld device	x					x		x	
Unauthorised use of social networking / instant messaging / personal email	x					x		x	
Unauthorised downloading or uploading of files	x				x	x		x	
Allowing others to access school network by sharing username and passwords	x				x	x		x	
Attempting to access or accessing the school network, using another student's / pupil's account	x				x	x		x	
Attempting to access or accessing the school network, using the account of a member of staff	x	x			x	x		x	
Intentionally corrupting or destroying the data of other users	x				x	x		x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x		x	

Continued infringements of the above, following previous warnings or sanctions	x	x	x			x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x			x	x	x	
Using proxy sites or other means to subvert the school's filtering system	x	x	x		x	x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x			
Deliberately accessing or trying to access offensive or pornographic material	x	x	x		x	x	x	x	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x	x	x	x	x	

Staff

Actions / Sanctions

Incidents:	Refer to Phase Leader	Refer to SLT / Headteacher	Refer to Local Authority / HR	Refer to Police/ ICO	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).		x	x	x	x			x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x	(x)			(x)			
Unauthorised downloading or uploading of files	x	(x)			(x)			
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	x	(x)			(x)			
Careless use of personal data eg holding or transferring data in an insecure manner		x		x				(x)
Deliberate actions to breach data protection or network security rules		x	x	x	x			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x	x			x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x		x			x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		x	x					x
Actions which could compromise the staff member's professional standing		x				x		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x				x		

Using proxy sites or other means to subvert the school's filtering system		x	x		x			x
Accidentally accessing offensive or pornographic material and failing to report the incident		x			x	x		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x			x
Breaching copyright or licensing regulations		x		x		x		
Continued infringements of the above, following previous warnings or sanctions		x	x	x			x	x

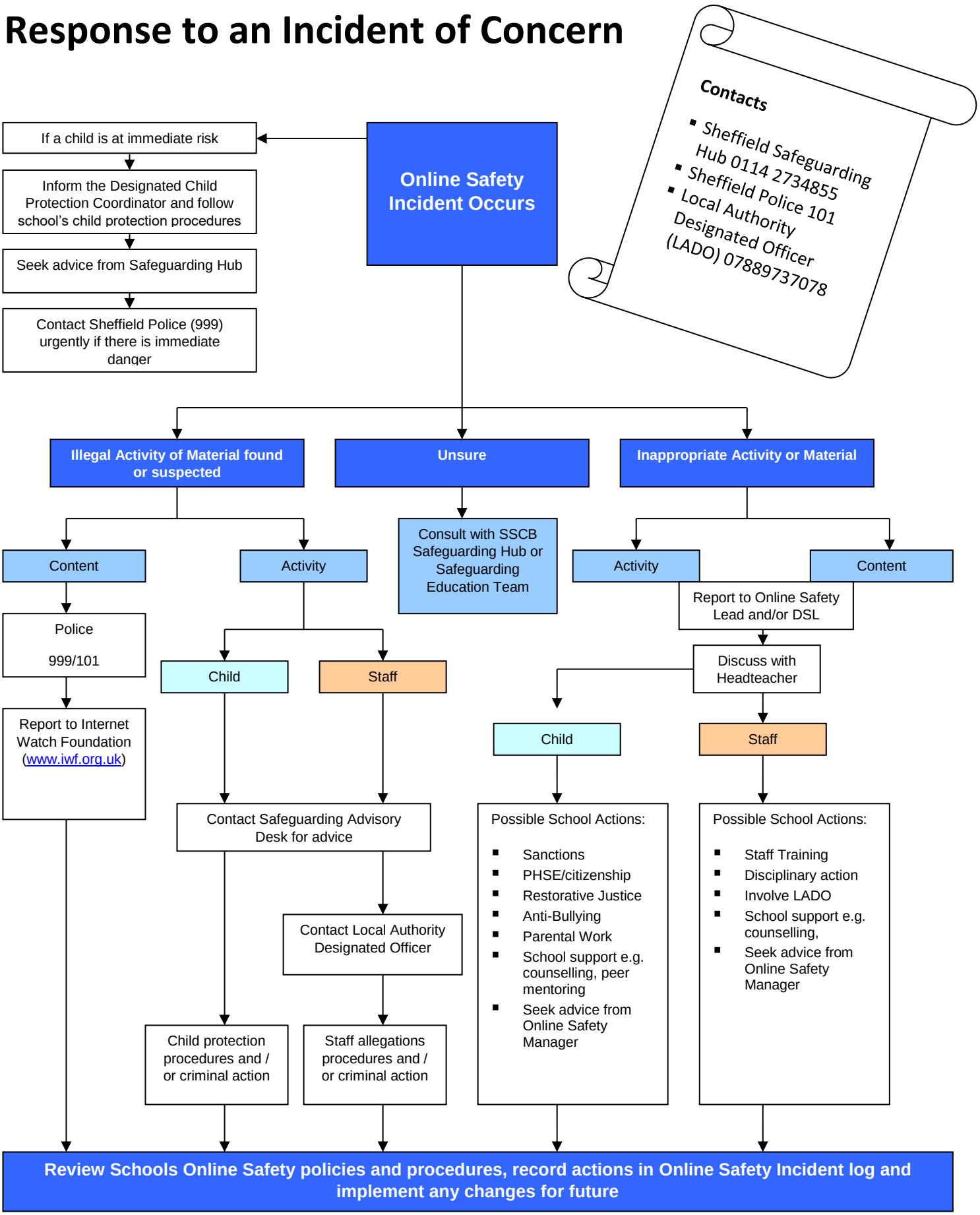
Dealing with Online Complaints

- Parents/Carers are reminded through communications at the start of each academic year of appropriate complaints channels and procedures.
- The complaints procedure is clearly detailed on the school website and within the Complaints Policy (www.oughtibridgeschool.co.uk).
- 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.

Appendices

- Response to an Incident of Concern Flowchart
- Pupil Acceptable Use Policy Agreements (FS/KS1 and KS2)
- Staff Acceptable Use Policy Agreement
- Volunteers and Visitors Acceptable Use Policy Agreement
- Parents /Carers Acceptable Use Policy Agreement
- Use of Digital Images Consent Form
- Mobile Phone Use Consent Form and Agreement
- Links to other organisations or documents
- Legislation

Response to an Incident of Concern



Contact Details

School's Designated Safeguarding Lead: Gemma Shelton
School Online Safety Coordinator: Stephi Dennis

FS AND KS1 ACCEPTABLE USE POLICY AGREEMENT

I will ask a teacher or suitable grown up if I want to use the computer or iPads.

I will only use activities that a teacher has allowed me to use.

I will take care of the computer and other equipment.

I know a password is private and will never share it with other people.

I will be polite and friendly with my words online.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me or worries me on the screen.

I know that if I break the rules I might not be allowed to use the computers or other equipment.

This agreement would be discussed and signed by children as a class.

KS2 ACCEPTABLE USE POLICY AGREEMENT

I will ask permission before using any ICT equipment or the Internet.

I will only use activities or websites that a teacher has allowed and know how to assess the reliability of different websites.

I will take care of the computers and other equipment and not change any settings without permission.

I will never share my username or password with other people, or try to use someone else's login details.

I will not take or share images of anyone without their permission.

I will be polite and friendly with my words online and encourage others to do the same.

I will ask for help from a teacher or suitable adult if I am not sure what to do, or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me or worries me on the screen.

I know that technology should be used in moderation and too much 'screen time' can be bad for my health.

I know that if I break the rules I might not be allowed to use the computers or other equipment.

Pupil name: _____ Class: _____

Pupil signature: _____ Date:_____

Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, digital cameras, smart watches, email and social media sites**.**
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (a strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system) and will change this periodically when prompted.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with General Data Protection Regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted by a method approved by the school. (For further details, refer to the Online Safeguarding Policy). Any images or videos of pupils will only be used as stated in the Online Safeguarding Policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school Online Safeguarding policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Gemma Shelton), the Data Protection Officers (Jim Dugmore / Catherine Askham) and the Online Safety Coordinator (Stephi Dennis) as soon as possible. I will report any accidental access, receipt of inappropriate

materials, filtering breaches or unsuitable websites to (Stephi Dennis) the Online Safety Coordinator, the designated lead for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider (Bluebox) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, smart watches, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school Acceptable Use policy and the Law.
- When using video communication with staff, parents/carers or pupils I will follow these procedures:
    - Wear suitable clothing – this includes others in my household
    - Be situated in a suitable 'public' living area within the home with an appropriate background
    - Use appropriate language – this includes others in my household
    - Use the necessary equipment and computer programs as intended
    - Not record, store, or distribute video material without relevant permissions
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.
- I will promote Online Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Online Safety Coordinator (Stephi Dennis) or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of ~~i~~nformation systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood the Staff ICT Acceptable Use Policy.

Signed | Date

Name

Parent/Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone including remote learning. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name(s)	
Pupil Name(s)	

As the parent/carer of the above pupil(s), I give permission for my child/children to have access to the internet and to ICT systems at school.

I know that my child/children has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child /children's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's Online Safety.

Signed Date

Volunteer ICT Acceptable Use Policy Agreement

As a professional organisation with responsibility for children's safeguarding, it is important that all volunteers take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All volunteers have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that volunteers are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, digital cameras, smart watches, email and social media sites**.**
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for volunteers use can only be used for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with General Data Protection Regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted by a method approved by the school. (For further details, refer to the Online Safeguarding Policy). Any images or videos of pupils will only be used as stated in the Online Safeguarding Policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school Online Safeguarding Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Gemma Shelton), the Data Protection Officers (Jim Dugmore / Catherine Askham) and/or the Online Safety Coordinator (Stephi Dennis) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Stephi Dennis) the Online Safety Coordinator, the designated lead for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider (Bluebox) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my role, whether using school or personal systems. This includes the use of email, text, smart watches, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my volunteer duties and will be in accordance with the school Acceptable Use Policy and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my role, the school, or the City Council, into disrepute.
- I will promote Online Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Online Safety Coordinator (Stephi Dennis) or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its necessary procedures. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood the Volunteer ICT Acceptable Use Policy.

Signed		Date	
Name			

Use of Digital Images Consent Form

The following paragraph forms part of the whole school permissions form which is sent to parents as part of their child's induction pack when starting school

Use of photographs and video

There are a number of occasions when the children will have their photographs and video footage taken during events and activities. Sometimes we like to include these on the school website, in the local press or other publications (e.g. termly colour newsletter). Although photographs and films can be shown freely within the confines of the school they cannot be made 'public' without your permission.

I do / do not* give permission for photographs/video images of my child to be used on the school website, Twitter, Facebook or other publication/s.

Your consent will be recorded on your child's school record through their life at Oughtibridge Primary School so you will not be asked for this again. If once returned you would like to amend the details you would need to put this in writing to the school office.

Mobile Phone Use Agreement and Consent Form

The following letter is sent to all Y4 and Y5 pupils in July of each year to gain consent before the start of the new academic year.

Dear Parents and Carers,

I am writing to you to outline our expectations regarding mobile phones/smart watches/fitbits with messaging facility. We understand that some children may need to have one of these devices and therefore would like to use this opportunity to explain what your child should do with it whilst in school.

We ask that the children turn off their device when they reach the school gates as they should not need to contact anyone when in the school grounds. We are responsible for the children when they are within the school grounds and would therefore be able to contact someone for them in an emergency. This also applies at the end of the school day. The children must hand their device into their class teacher at the start of the school day where it will be kept in a box until the end of the school day.

Photographs should not be taken on devices by anybody when within the school grounds. We have a photograph policy in school and not all children have been given permission to have their photographs taken. If there is any time that your child may need to turn their device on whilst still in the school grounds then please ask your child to talk to their class teacher about this first.

In anticipation of your child moving into Y5 or Y6 from September if you would like your child to have a messaging device in school please complete the slip below. This slip also outlines that we as a school accept no responsibility of any device whilst on school property.

Yours sincerely

Mr Jim Dugmore
Headteacher

Mobile Phones in School

Name of child _____ Class _____

- ☐ I give permission for my child to bring a mobile phone/smart watch/fitbit with messaging facility/other (please state) to school.

  Please give reasons for this. _____
  _____
  _____

- ☐ I understand that the school accepts no responsibility for any devices whilst on school property.

Signed _____ Date _____

Links to other organisations or documents

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

General

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.

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.

General Data Protection Regulations 2018

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. GDPR states that personal 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.

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 Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

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

Sexual Offences Act 2003

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 / 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.