



Thrupp Primary School

Internet Safety & Acceptable Use Policy

Approved by: Standards and Welfare	Reviewed: November 2025
Last Reviewed: November 2024	Next review due by: November 2026

Contents

1. Introduction	3
2. Roles and Responsibilities	5
3. Technical – Infrastructure/Equipment, Filtering and Monitoring ...	9
4. Teaching and Learning.....	11
5. Training and Awareness Raising	13
6. Use of digital and video images	14
7. Responding to Incidents of Misuse:.....	15
8. Data Protection and Copyright.....	22
9. Staff (and Volunteer) Acceptable Use Agreement	24
10. Parent/Carer Acceptable Use Agreement.....	28
11. KS1 Acceptable Use Agreement	32
12. KS2 Acceptable Use Agreement	33

Thrupp Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff, governors and volunteers to share this commitment.

1. Introduction

This policy should be read alongside Thrupp Primary School's policies and procedures on child protection, anti-bullying, safeguarding and code of conduct for staff and volunteers.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of the school. This policy has been developed by the Computing Leads (Mrs R Lewis & Mr J Muskett) in consultation with the SENCO, senior leadership team, teachers and governors. Updated guidance and pupil/parent/staff voice questionnaires have shaped and will continue to help shape this policy and learning in school around internet safety. This policy is also based on government recommended/statutory programmes of study.

The governors will receive a report about internet safety in our school once a year. The online safety policy will be reviewed annually, or more regularly in light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place.

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 is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The aims and purpose of this policy:

We understand the immense value technology and the internet play not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school. We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all pupils.

We therefore understand the importance that using the internet has for education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these, however we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Principles:

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

However, the use of these technologies can put young people at risk within and outside the school. The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

Some of the dangers children may face include:

Content, access to illegal, harmful or inappropriate images or other content, access to unsuitable video/internet games, an inability to evaluate the quality, accuracy and relevance of information on the internet and the potential for excessive use which may impact on the social and emotional development and learning of the young person.

Contact – This may involve the risk of being subject to grooming by those with whom they make contact on the internet, inappropriate communication/contact with others, including strangers, cyber-bullying and identity theft.

Conduct – This may involve unauthorised access to/loss of/sharing of personal information, digital footprint and online reputation, the sharing of personal images without consent or knowledge, plagiarism and copyright infringement and illegal downloading of music or video files.

Many of these risks reflect situations in the off-line world. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks of which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

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

Our aims:

- Provide an exciting, rich, relevant and challenging Computing curriculum for all pupils.
- Enthuse and equip children with the capability to use technology safely throughout their lives.
- Teach children to become responsible, respectful and competent users of data, information and communication technology.
- Teach pupils to understand the importance of governance and legislation regarding how information is used, stored, created, retrieved, shared and manipulated.

- Equip pupils with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise the risk to themselves and others.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that we operate in line with our values and within the law in terms of how we use online devices.

How we do this in our school:

Online safety has a high profile at Thrupp Primary School for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6 and embedded in learning.
- A curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- We form strong 'parent partner' relationships through our home/school links and communication channels and parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.

Legal Framework:

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/online-abuse/>
- bullying <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/>
- child protection <https://learning.nspcc.org.uk/child-protection-system>

2. Roles and Responsibilities

Internet Safety is recognised as an essential aspect of strategic leadership in Thrupp School and the Headteacher and Online Safety Lead, with the support of Governors, aims to embed safe practices into the culture of the school. We ensure our appointed Online Safety Lead has an up to date knowledge of current practice and issues.

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online Safety Governor. **The role of the Online Safety Governor will include:** (Mr P Auton)

- Regular meetings with the Online Safety Lead
- Regular monitoring of online safety incident logs
- Reporting back to Governors in relevant meetings

The role of the Headteacher and Deputy Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher is also the Designated Safeguarding Lead and our Deputy Headteacher is our Deputy Designated Safeguarding Lead. They are trained in online safety issues and aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming and cyber-bullying.
- The Headteacher and Deputy Headteacher are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Governors should take part in online safety training/awareness sessions too.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher will receive a formal monitoring report once a year from the Online Safety Lead and regular monitoring reports from our IT technical support.
- The Headteacher, Deputy Headteacher and all teaching staff should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures)
- The Headteacher will inform the local authority about any serious online safety issues including filtering.
- The Headteacher will ensure that the school infrastructure/network is safe and secure and that policies and procedures approved within this policy are implemented.

Online Safety Lead: (Mr J Muskett)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school’s online safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and/or broker relevant training and advice for staff.
- Liaises with school technical staff and the local authority when necessary.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments with support of the Headteacher.
- Meets with Online Safety Governor to discuss current issues, review incident logs and filtering.
- Reports regularly to Headteacher and governors.
- Develop an online safety teaching programme to deliver the statutory programme of study.
- Monitor online safety teaching to ensure this is being delivered and is having an impact on pupils’ understanding.

Technical staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering is robust in blocking, but does not inhibit learning and teaching.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher, Chair of Governors or Online Safety Lead for investigation/action/sanction.
- that monitoring software/systems are implemented and updated.
- all security updates are applied (including up to date anti-virus definitions, windows updates) and take action to prevent spyware and malware.
- there are regular reviews and audits of the safety and security of school ICT systems.
- servers, wireless systems and cabling are securely located and physical access is restricted.
- all users have a clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.
- the school infrastructure and individual workstations are protected by up to date virus software.
- that a software licence audit is regularly updated and also making regular checks to ensure that the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional licence costs.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety issues and of the current school's online safety policy and practices.
- they have read, understood and signed the staff acceptable use agreement and act in accordance with this and the Online Safety Policy.
- they report any suspected misuse or problem to the Headteacher and Online Safety Lead for investigation. In the event that the incident involved the Headteacher, report to the governor responsible for safeguarding.
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy and their agreement.
- the planned programme of study for online safety is delivered through their teaching.
- a planned programme of formal online safety training will be made available to staff.

- they deliver the scheme of work for online safety and ensure children have a good understanding of what is being taught.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc. in school (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use, that pupils are aware of how to search safely and that any unsuitable material that is accessed is dealt with according to school policy.
- immediately report any issues in accordance with school policy.

Staff should be aware that many seemingly innocuous Internet sites and Internet-connected services/applications include social media components that could expose pupils to risk and that this should be taken into consideration when tasks are being introduced in class that might be repeated at home. This might include leaving reviews or comments on websites or playing multiplayer online games. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Internet Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Designated Safeguarding Lead:

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issue to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber bullying

Pupils:

Pupils are responsible for using the school's digital technology systems in accordance with the pupil acceptable use agreement. Pupils are also expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with Internet safety issues, both at home and school.

- Must practice age-appropriate safe searching in order to reduce access to unsafe material.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of abuse, misuse or access to inappropriate materials, know how to do so and do this immediately when an issue arises. This understanding will enable them to have the confidence to ask an adult for clarification if they are unsure.
- Will be expected to know and understand policies on the use of mobile phones and digital cameras. They should also know and understand policies on the taking/use of images and on cyber bullying.

- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership to the school.
- Help their friends to keep safe by pointing out any risks and what they could do about them.

Parents/Carers:

We hope to form strong 'parent partner' relationships with parents to ensure we work together to support our children. Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information about national or local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice. It is the responsibility of parents and carers to:

- Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe.
- Follow the school policy and requests regarding digital and video images taken at school events. We request that digital images and videos that have other children in should not be shared online, such as on social media sites, for safeguarding reasons.
- Endorse by signature the Pupil Acceptable Use Policy.
- Ensure that their child/children follow appropriate agreement rules at home.
- Discuss online safety issues with their child/children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet.
- Keep up to date with issues through school updates and attendance at events.
- Ensure their children follow the rules on appropriate use of children's own devices in school.
- Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use them to inform any changes to teaching.

Community Users:

Community users who access school systems as part of the wider school provision will be expected to sign a Community User agreement before being provided with access to school systems.

3. Technical – Infrastructure/Equipment, Filtering and Monitoring

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. SWGfL provide the internet and filtering system.

- There will be reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.

- All users will be provided with a username and password by IT technical support who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system, used by IT technical support, must also be available to the Headteacher and kept in a secure place.

Filtering and monitoring systems are in place for all our online access. We use the SWGfL, which is a sophisticated content filter, to ensure that as far as possible only appropriate content from the internet finds its way into school. Whilst the filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. If this happens pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. Teachers and staff users are able to bypass the filtering service in order to access some resources that are filtered for learners so as to ensure that 'over blocking' does not restrict teaching.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff can monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for staff or pupils to report any actual/potential technical incident/security breach to the relevant person.
- 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. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place that a login name is set up for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data should not be sent over the internet access unless going to and from a 'thrupp.gloucs.sch.uk' email address or using Egress when emailing professionals in the local authority. Office 365 systems are encrypted should personal data need to be shared, although staff should consider carefully how much data to pass on.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.
- Staff are only allowed to install programmes on school devices when approved by our technical support.

Portable storage media

Staff are allowed to use their own portable media storage (USB Keys etc.). If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT technicians. Personal data cannot be taken off the school site unless safely encrypted or otherwise secured.

Communications

A wide range of rapidly developing communication technologies has the potential to enhance learning and management. Our school considers the benefit of using these technologies for education outweighs their risks/disadvantages. Staff are allowed to bring their own mobile phones to school that can be used during their own free time. Parents may request that personal mobile phones are kept in school for pupils who may need them on their journey to and from school. These must be given to the school office at the beginning of the school day and will be returned to the pupil at the end of the day. The school cannot accept responsibility for any loss or damage of these devices.

When using communication technologies Thrupp Primary School consider the following as good practice:

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications may be monitored.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in any nature and must not respond to any such communication.
- Governor communications take place through governor school email accounts. Personal or sensitive information is not emailed.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community.
- Personal opinions are not attributed to the school.
- Security settings on personal social media profiles are advised to minimise risk.
- Personal data should not be sent over the internet access unless going to and from a 'thrupp.gloucs.sch.uk' email address or using Egress when emailing professionals in the local authority. Office 365 systems are encrypted should personal data need to be shared, although staff should consider carefully how much data to pass on.

4. Teaching and Learning

The Online Safety curriculum at Thrupp Primary School is built around the statutory content of the 2014 National Curriculum and Early Years Foundation Stage Curriculum.

Computing is a foundation subject; the National Curriculum programmes of study include:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

We believe it is our responsibility to prepare pupils for their lives in the modern world, and computing is an integral part of that world. At Thrupp School we are committed to teaching pupils to use ICT effectively and appropriately in all aspects of their education.

- We have a planned online safety curriculum as part of our Computing lessons which is revisited at the start of every term.
- Key online safety messages are reinforced as part of a planned programme of assemblies and activities.
- Pupils are taught in all lessons to be critically aware of materials and content they access online and in Key Stage 2 they are guided to validate the accuracy of information.
- Key Stage 2 pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making.
- Pupils sign and are helped to understand the acceptable use agreement and encouraged to adopt safe and responsible use both within and outside our school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- It is best practice that pupils are guided to sites checked as suitable for their use by staff members. However, where pupils are freely searching on the internet, staff are vigilant in monitoring the content of the websites they visit.
- We have a Teaching and Learning policy (see separate policy) which outlines clear expectations of home learning online and the use of our chosen online learning platform.

Rules for keeping safe are reinforced with the acceptable use agreement that pupils sign and parents are communicated this also so they can reinforce the messages at home. All classes have online safety posters displayed in their classroom and staff regularly refer to these. Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved. Safer Internet Day in February will be used every year to promote the importance of being safe and responsible users of technology.

At the beginning of every school year, all pupils, parents, staff and volunteers will be given a copy of the appropriate Acceptable Use Agreement to sign so they are aware of the rules and sanctions. Pupils' agreements are also signed by the parent as well to make sure that the rules have been discussed.

Early Years Foundation Stage:

Within the EYFS, the specific areas of 'Personal, Social and Emotional Development' and 'Understanding the World' help children to develop a positive sense of themselves and others; form positive relationships and develop respect for others; develop social skills and

learn how to manage their feelings; understand appropriate behaviour in groups; and to explore, observe and find out about people, places, technology and the environment.

Continuous provision is resourced to ensure that pupils are given the opportunity to explore the world around them and how technology can be used to support their exploration.

Use of the Internet by pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. **Pupils are always actively supervised by an adult** when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

Out of Hours Provision

There is an after-school and a breakfast club that runs each day. There will be no unsupervised access to the Internet at any time during our out of hours provision. Our school staff has compiled a list of approved and acceptable games and websites that the children can use during this provision. Out of hours staff ensure these are the only sites they access during this time.

5. Training and Awareness Raising

All staff, including support staff, receive an annual online safety update as part of our Safeguarding training in September INSET and training. Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues. The Online Safety Lead provides advice and training as required to individuals and seeks LA advice on issues where appropriate. A training log is used to record when updates and training are delivered.

Induction Processes:

All new staff receive online safety training as part of their induction programme. Parents of new reception children receive information about online safety and processes when their child starts school. There are also updates to this throughout the key stages. Parents of children who join school mid-year are provided with an overview of expectations linked to relevant policies including online safety and their children are also introduced to the acceptable use policy.

Parents/Carers:

Parents and carers have an essential role in educating their children and monitoring their behaviour online; however, they may have a limited understanding of the risks and issues and underestimate the dangers or be unsure of how to deal with them. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure how to respond. Our school staff form strong relationships with parents and will help parents understand these issues through newsletters, letters, website updates and information about national/local online safety campaigns.

Education and Training of Staff and Volunteers:

It is essential that all staff receive online safety training so that they understand their responsibilities, as outlined in this policy. All staff, including support staff, receive an annual online safety update as part of our Safeguarding training in September INSET. An audit of the online safety training needs of all staff will be carried out as required and any additional training provided to suit. All new staff should receive online safety training and training on relevant policies as part of their induction programme. Policies relevant to online safety and their updates are discussed at staff meetings. The Online Safety Lead will provide advice/guidance/ training to individuals as required.

Governors:

Governors should take part in online safety training/awareness sessions, with particular importance for those who are involved with technology and safeguarding. This may be offered through regular newsletter information and access to website information, participation in school training/information sessions for staff or parents and attendance to training provided by outside agencies.

Special Educational Needs and Disabilities:

Children with SEND will be supported in line with the SEND Policy. Where barriers to learning are identified, the class teacher will work closely with the SENDCo to ensure difficulties are addressed and a programme of learning is put in place to support the child to close the gap. Where necessary, children may access intervention groups to support the development of basic skills.

6. Use of digital and video images

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyber bullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images/videos of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. Their photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment or when used on personal equipment it should be deleted as soon as possible after it has been used.
- Staff give permission to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied.

- Images are only taken and used of individuals where there is a signed permission in place.
- Pupils full names are not published on any online platform or school communication including the website and newsletter. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are able to take videos and digital images of their children at school events for their own personal use as this is not covered by the General Data Protection Regulation. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents/carers should also not comment on any activities involving other pupils in the digital/video images.
- Pupils' work is only published with no identifiers other than the pupils' year group/class name or first names.
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

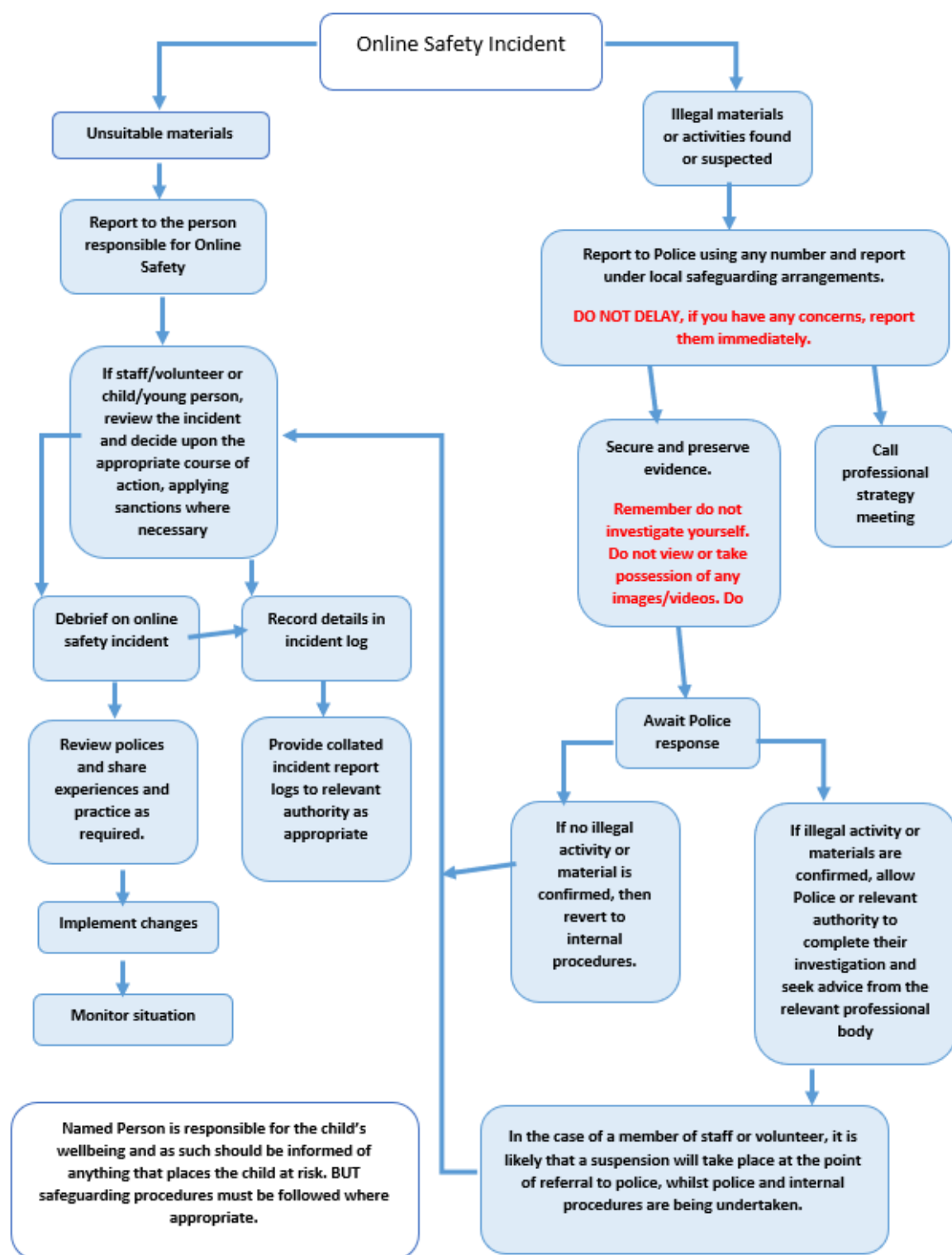
7. Responding to Incidents of Misuse

Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules are displayed in each classroom. Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this will be reported immediately to the police. Please refer to the right hand side of the flowchart below.



Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure will be followed:

- Have more than one senior member of staff involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure but also that the sites and content visited are closely monitored and recorded.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement of Local Authority
 - Police involvement or action
- If content being reviewed includes images of child abuse, then the monitoring will be halted and referred to the Police immediately. Other instance to report to the police would include:
 - Incidents of 'grooming' behaviour
 - The sending of obscene materials to a child
 - Adult material which potentially breaches the Obscene Publications Act
 - Criminally racist material
 - Promotion of terrorism or extremism
 - Offences under the Computer Misuse Act
 - Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

How will complaints regarding Internet safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. It is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. The Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is also referred to the Headteacher. See table overleaf for further details.

Pupils Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X	X					X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X			X		X	X
Unauthorised/inappropriate use of social media/messaging apps/personal email	X	X			X		X	X
Unauthorised downloading or uploading of files	X	X		X	X		X	X
Allowing others to access school network by sharing	X	X					X	X

username and passwords								
Attempting to access or accessing the school network, using another pupil's account	X	X			X		X	X
Attempting to access or accessing the school/academy network, using the account of a member of staff	X	X			X	X	X	X
Corrupting or destroying the data of other users	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X			X	X		
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	X	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		X	X
Deliberately accessing or trying to access offensive or pornographic material	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

Staff Incidents	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).	X	X	X				
Inappropriate personal use of the internet/social media/personal email	X			X	X		X
Unauthorised downloading or uploading of files	X			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		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X		
Deliberate actions to breach data protection or network security rules	X	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 message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils	X	X			X	X	X
Actions which could compromise the staff member's professional standing	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
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
Breaching copyright or licensing regulations	X				X		X

Continued infringements of the above, following previous warnings or sanctions	X	X					X	X
--	---	---	--	--	--	--	---	---

8. Data Protection and Copyright

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

- The school has data protection policy in place (please see separate documentation for more details) and is able to demonstrate that it implements these data protection principles.
- Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.
- Staff understand that there are complex copyright issues around many online resources and materials.
- We have a Data Protection Officer (DPO) who has high level of understanding of data protection law and is free from any conflict of interest. (Mrs C Tyler-Sell – Headteacher at Nailsworth Primary School)
- The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Our Data Protection policy sets out how to deal with FOI requests. See this policy for more details.
- All staff receive data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written.
- Access personal data sources and records 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.
- If storing data on any portable computer system or memory stick, the data must be encrypted and password protected. It must be securely deleted from the device, in line with the school policy once it has been transferred or its use is complete.

Thrupp Primary School Staff (and Volunteer) Acceptable Use Agreement

Context

Technologies and the internet, including social media, are powerful tools which provide excellent opportunities for learning and teaching. They can motivate learners, promote creativity, and support effective learning, assessment and engagement with parents. They also bring opportunities to enhance teaching, increase staff efficiency and provide opportunities for staff to benefit from professional development through networking and collaboration. All users have an entitlement to good, safe access to ICT and the internet. This policy relates to use of all technologies including mobile phones, tablets and online services such as social networking sites.

It is intended to ensure that:

- Staff and volunteers are responsible users and stay safe while using technologies.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.
- The organisation is protected from any issues that could negatively affect its reputation.

Content

- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I know that internet use is proactively monitored and any illegal activity will automatically result in police involvement.

Contact

- I will communicate online in a professional manner and tone and I will not use aggressive or inappropriate language and am aware that any communication could be forwarded to an employer or governors.
- I will only communicate with students / pupils and parents / carers using official school systems or those that have been approved by the Headteacher.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily.

Social Media

- I will only use chat and social networking sites (for school purposes) that are approved by the school.
- When using social networking sites and other services for personal use I will not say anything that could bring the school, staff members or any member of the school community into disrepute.

- I will not engage in any online discussion about the school or any members of the school community unless this is in an approved context e.g. school own Twitter account.
- I will not attribute my personal opinions to the school on sites and will make clear that they are my own opinions.
- I will immediately report any online discussion that could impact on the school / staff reputation and any negative postings about any member of the school community
- I will not 'friend' current pupils on social networking sites.

Conduct

- I will only use school equipment for the purposes of learning and teaching unless otherwise approved by the Headteacher.
- I will not engage in any online activity that may compromise my professional responsibilities or compromise the reputation of the school or its members. This includes use of the school e-mail account, logo or my school role.
- Filtering is provided through the SWGfL. I know that, as a staff user, I have access to resources that learners cannot access for teaching purposes.
- I will not try to access sites that are illegal.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement when using it.
- I will only take images or video of pupils/staff where it relates to agreed learning activities and will ensure I have parent/staff permission before I take them. If these are to be published online or in the media I will ensure that parental / staff permission allows this.
- Where images are published (e.g. on the school website) I will ensure it is not possible to identify the people who are featured by full name or other personal information.
- I understand my photograph may be used on the school website, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details.
- I will not install or store programmes on a school device unless I have permission.
- I will not try to alter computer settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school and will immediately report any damage or faults involving equipment or software.
- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Data Protection

- I understand that our school only uses services which mean that data is stored in line with EU guidelines.
- When I use my staff laptop at home I will ensure resources cannot be accessed or copied by anyone else and that no one else uses the laptop.
- I will ensure personal equipment used is password protected.
- I will ensure that my data is regularly backed up.

- I will take all steps within my power to keep personal data safe and minimise the risk of losing it.
- I will only use personal data on secure devices that are password protected.
- When transferring data I will use encryption and secure password protected devices.
- I will ensure that devices I use have approved virus and malware checking software and I will delete data securely once it has been transferred or finished with.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when I am required by law or by school policy to disclose it to an appropriate authority.
- I will not send personal information by e-mail as it is not secure unless this is via egress or between school email addresses.

Promoting Safe Use by Learners

- I will model safe use of technologies and the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in or out of school that might compromise learner, user or school safety; or if a child reports any concerns.
- I will monitor learner behaviour online when using technology and deal with any issues that arise.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety of other staff and pupils or to the security of the ICT systems. I understand that these rules are in place to enable me to use ICT safely and that if I do not follow them I may be subject to disciplinary action. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT if allowed (including mobile phone or tablet) in school
- I use my own ICT out of school (including mobile phone or tablet) to use school sites or for activities relating to my employment by the school. I know that the school will monitor my use of the school ICT systems and communications.

Problems

- I will immediately report any illegal, inappropriate or harmful material; or incident I become aware of, to the online safety lead or head teacher.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the head teacher.
- If I believe a young person may be at risk I will follow the child protection procedures.
- If I believe a young person may be being bullied I will follow the anti-bullying procedures.

Use of Staff Images on School Publicity and Websites

I understand my photograph may be used on the school web site, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details other than my title and surname.

Staff / Volunteer Name:**Signed:****Date:**

Thrupp Primary School Parent / Carer Acceptable Use Policy Agreement

Technologies open up new learning opportunities and can promote creativity, effective learning collaboration and communication. They can promote more effective communications between parents / carers and the school in order to support young people with their learning. This policy relates to use of all technologies including mobile phones, tablets and online services such as learning platforms and online communications. This Acceptable Use Policy is intended to ensure:

- You are aware of what the school is doing to help your child become a responsible user of technology and stay safe at school.
- You are aware of the importance of e-safety and are able to support your child with keeping safe and behaving well online at home. The school will aim to ensure your child has good, safe access to ICT for learning and, in return, expects your child to use the equipment responsibly.

Content

The school takes every reasonable precaution, including monitoring and filtering systems, to ensure that your child is safe when they use technology at school. The school cannot be held responsible for the nature and content of all materials that are accessible, using technology as security systems cannot protect against everything. We teach children about the risks of using technology and how to keep themselves safe.

- We only allow children to use age appropriate websites in school, as using sites for older users can increase the risks to them. This includes social networking sites like Facebook, where the terms and conditions require users to be 13. We appreciate that some parents may allow their children to use sites that they are not old enough for at home. If this is the case, then you will need to monitor their use and deal with any issues that arise.
- We prevent the use of age inappropriate online gaming sites in school as these can contain adult content and also enable adults to make contact with children online.

Contact

School policy requires that staff only make contact with parents or children through agreed school systems. This being the case we hope you will respect this by not requesting to be friends with staff on social networking sites and will understand if staff refuse any friend requests that are made.

- We limit the ability of children to contact each other online in school and use only tools where contact can be limited to others in our school community.

Conduct

- Your child is expected to behave well online as they are expected to during all other school activities.
- Your child will be asked to sign an Acceptable Use Agreement which sets out clear expectations of behaviour when working online. We hope you will talk to your child about this.
- Bullying is not tolerated in any form and this includes online (cyber-bullying). Any instances of this will be dealt with as detailed in our Anti-Bullying and Hate Policy.

- Your child will be taught about online safety and how to keep safe when using technology.
- They should only use their own log in for systems and to keep their details private. Your child is responsible for anything their log in is used for.
- Your child's use of ICT in school will be monitored and we will contact you if we have e-safety concerns.

Taking Digital Film and Images

- Children and staff may use digital cameras to record learning activities. These images may be used in lessons or to celebrate success through being published in newsletters, on the school website or occasionally in the public media.
- The school will comply with the General Data Protection Regulation and ask your permission, through this policy, before taking images. We will also ensure that when images are published the young people cannot be identified by the use of their names.
- In line with guidance from the Information Commissioner's Office, parents / carers may take videos and digital images of their children at school events for their own personal use as this is not covered by General Data Protection Regulation. These images must not be published or made available on social networking site in order to protect other children and respect privacy. Parents / carers should also not comment on any activities involving other pupils in the digital / video images.

Problems

- We can only take responsibility for e-safety issues that happen in school or at home when children are using sites recommended by the school.
- Any issues you are made aware of with use of technology in school should be reported immediately to a child's teacher so that appropriate steps can be taken.
- If your child does not behave appropriately online then the school will take steps to deal with this as with any other issue with behaviour.
- You are obviously responsible for your child's safety online when at home and we would hope you will be discussing e-safety with your child and monitoring their use of computers and mobile phones.
- If there is an issue occurring outside school that it may be helpful for us to be aware then please let your child's teacher know. While we do not have responsibility to resolve all issues, we may be able to deal more effectively with any implications happening in school and adapt our teaching programme to ensure that these issues are covered.

Permission Form

We request that you sign the permission form below to show your support of the school in helping to keep your child safe. By signing this form you are agreeing that:

- Your child can use school technology and online services for learning.
- You have read and discussed the rules with your child.
- You understand the rules that your child should be following when using ICT in school and this also applies to their use of their mobile phone

Parent / Carers Name:

Date:

Student / Pupil Name:

Home Use of the Internet

We hope you will reinforce the e-safety messages when your child uses the internet at home. Some ways that you could do this are listed here to support those of you who may not be aware of all the issues. With the large number of mobile devices it is now very difficult to supervise all access to the internet, however you will want to set age appropriate rules for using technology at home. The school rules could be a starting point.

Content

- Make sure content is appropriately filtered for younger users.
- Make sure your child knows that a protection system does not stop all unsafe content and they need to tell you if they access something inappropriate or get an upsetting message.

Contact

- Talk about the need to be polite online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including parents, head teacher or future employer!).
- Make sure they know they should not open messages if the subject field is offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
- Ensure that any online games they are using are of an appropriate age rating and make sure they are aware that they could be contacted through games and not to give out personal information.

Conduct

- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only post things they would be happy for anyone to read.
- Check that they are old enough for the sites they are using. If you allow them to use a site they are not old enough for ensure that you have access to what they are doing so that you can monitor it.
- Make sure that family computers are password protected and have anti-virus software which is regularly updated.
- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them.
- Discuss user names and talk about how to choose them carefully to protect their identity.
- Talk about the information children should keep private in order to stop them being contacted including full name, direct e-mail, address, telephone number, school and places they go regularly. Check information that younger users are publishing to ensure that they are not putting themselves at risk. This includes any personal information which could lead to someone being able to contact them.
- Ask your child about the sites they are visiting.
- Talk about using the safety and privacy features of sites to only give access to people they know and to be careful who they add as friends.

- Make sure they know that downloading copyrighted games and music without paying for it is illegal.
- Remind them they should not respond to offers they have not requested as these could be scams, result in costs or be trying to find out their personal information.
- Remind them that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Problems

- Make sure they know that if they get any problems with using computers or get an offensive or worrying message / e-mail they should not reply but should save it and tell you.
- Please tell the school of any concerns that you have or anything that they could help to address through teaching.
- **Reassure your child that if they talk to you about a problem online you will not ban them from going online as this will discourage them from telling you.**

Thrupp Primary School KS1 Acceptable Use Agreement:

How to keep me safe at home and at school:

✓ We check with a grown up before using the internet.



✓ We tell a grown up if something we see makes us feel worried.

✓ If we get stuck on the internet we will ask for help. If we see something upsetting, I will close it down and tell an adult straight away.



✓ We can write polite and friendly messages to people we know. We will not send or write anything that may upset somebody else.

✓ We will keep our personal information (our name, address, school, pictures) "TOP SECRET" and not share them on the internet.

X We must not download anything without permission from an adult.



X I must not use other people's work as my own.

X I must not pretend to be anyone else.



Pupil's agreement:

If you do not follow the rules you might lose access to the computers. The school will regularly check what you are doing on the computers. If you understand the rules please sign your name below:

.....

And ask your parent/carer to sign below:

Signed: _____

Date: _____

Please print name: _____

Relationship to the child: _____

Child's name: _____

Thrupp Primary School KS2 Acceptable Use Agreement:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush - I will not share it, nor will I try to use any other person's username or password.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share any personal information about myself or others when online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others.
- I will not take or share pictures or photographs of anyone without their permission.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will ask permission before using any ICT equipment and will only use it when a teacher or another adult is with me.
- I will also ask permission before using the internet and will only go on websites I have been told to go on by an adult.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I will not send anyone material that could be considered threatening bullying, offensive or illegal.
- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate use of ICT or if I fail to comply with this agreement.
- If I am concerned about anything I see on the internet or any messages that I receive I know that I can talk to my class teacher, head teacher, parents and any other staff members.

Pupil's agreement:

I have read and understand the above and agree to follow these guidelines when using the school ICT systems and equipment whether at home or in school. Sign your name below:

.....

And ask your parent/carer to sign below:

Signed: _____ Date: _____

Please print name: _____

Relationship to the child: _____