HUNDON AND THURLOW PRIMARY FEDERATION

Laying the foundations for a bright future

The Parable of The Wise and The Foolish Man
(Matthew, Chapter 7, verses 24 to 27 and the Gospel of Luke, Chapter 6, verses 46 to 49)

Online Safety Policy
(including Acceptable Use of ICT and Mobile Devices)

NB: This policy has been discussed and considered for equality giving consideration to the protected characteristics- gender, age, race, disability, religion or belief, sexual orientation, gender reassignment, pregnancy or maternity and any other recognised area of discrimination.

Reviewed: Autumn 2020

Date of review: Autumn 2022

Approved by Headteacher and Safeguarding Governor

Signature of Chair of Governors:

Co-Chairs of Governors

Aims

This policy aims to explain how staff, volunteers, governors, parents/carers and children can all be part of online safety and are educated to be safe and responsible users capable of making good judgements about what they see, find and use.

This policy:

- Emphasises the need to educate staff, volunteers, governors, parents/carers and children about the pros and cons of using new technologies both within and outside school.
- Provides safeguards and an agreement for acceptable use to guide all users, whether staff or pupil.
- Ensures adults are clear about procedures for misuse of any technologies both within and beyond school and minimises the risk of litigation
- Develops links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

This policy applies to all ICT/Computing facilities and devices in our schools and use of school equipment outside of school and for all school based business and communications. It also covers personal devices brought onto the school premises, for example mobile phones.

Roles and Responsibilities

Governors/ Headteacher/School Leadership Team

The governing body is responsible for ensuring that employees act in a lawful manner, making appropriate use of school technologies and their own personal devices. It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher is the Online Safety Lead. They implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT/Computing learning environment.
- The ICT/Computing Leader is responsible for promoting online safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan and ensures that all staff receive adequate training and induction to implement this policy.
- The Federation has engaged a Data Protection Officer for both schools; they ensure compliance with the General Data Protection Regulation (GDPR) and current Data Protection legislation. They implement policies, procedures and staff training in this regard.
- Governors are informed via Teaching and Learning meetings about the progress of or any updates to the online safety curriculum.
- Governors ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all online safety guidance and practices are embedded.
- The Safeguarding Governor is also the online safety governor. Their role is to challenge the school about having Acceptable Use Policies with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT.
- Governors ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.
- Staff found in breach of this policy will be disciplined in accordance with school disciplinary procedures. In certain circumstances, breach of this policy may be considered gross misconduct

resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.
- The Headteacher is responsible for maintaining an inventory of ICT/Computing equipment and a list of school laptops, iPad and mobile devices and to whom they have been issued. A physical check of the inventory is carried out by the Admin team.

Managing Allegations:

Allegations made against a member of staff should be reported to the Designated Safeguarding Lead (DSL) for safeguarding within the school immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO)

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Local Online Safety Lead

It is the role of the Designated Online Safety Lead to:
- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe learning environment within the school.
- Ensure that this policy is reviewed, with up-to-date information and training available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and children in the initial set up of a network, stand-a-lone PC, staff/children laptops and iPads (other tablets and mobile devices) and ensure the technician is informed and carries out work as directed. Ensure that all adults are aware of filtering levels and why they are there to protect children.
- Liaise with the PSHEE, safeguarding and ICT/Computing leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct online safety information can be taught or adhered to.
- Ensure there is transparent monitoring of the Internet and online technologies:
    - Prompt reporting of issues
    - Encouraging use of monitored or recommended sites
    - Subscribing to educational web based curriculum services, updated through a proxy server
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Managing Allegations Procedure from the SSCB to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Ensure there is appropriate, up-to-date anti-virus software and anti-spyware and that this is reviewed regularly.

Staff/Adults – use of ICT

- No user shall access (e.g. read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law, other than the monitoring of acceptable use by School Management.

- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- Users are required to protect their password and not share their account details with others for their use, nor utilise another user account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.
- Users must not load or download software or Apps on any device without the authorisation of the Headteacher. Periodic audits of software and Apps will be undertaken.
- Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops. Any transfer of sensitive information should only be made via an encrypted memory sticks.
- Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.
- Ensure that all personal storage devices (i.e. memory sticks/portable hard drives) which are utilised by staff members to hold sensitive information are encrypted or password protected with either fingerprint technology or 6 digit passcode lock in the event of loss or theft.
- Websites should not be created on school equipment without the written permission of the Headteacher.
- All users sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school. By logging on to ICT systems, users agree to abide by this policy.
- Users may access school emails via personal mobile devices (i.e. iPad or mobile phone) providing the mobile device is protected with either fingerprint technology or 6 digit passcode lock.
- Staff when working from home will only use school supported devices for storing data, and will endeavour to save data to a cloud based system or an encrypted device.

Staff/Adults (Online Safety)

- All users are expected to act in a responsible manner, with the clear understanding that all information may be accessible to the public and under the Freedom of Information Act 2000. Privacy and confidentiality is in accordance with the current Data Protection legislation, the Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The County Council or school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:
    - There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
    - An account appears to be engaged in unusual or unusually excessive activity
    - It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability.
    - Establishing the existence of facts relevant to the business.
    - Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
    - Preventing or detecting crime
    - Investigating or detecting unauthorised use of ICT facilities
    - Ensuring effective operation of ICT facilities

    - Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
    - It is otherwise permitted or required by law.
    - In any instances where a child accesses inappropriate web pages or other internet media (i.e. inappropriate for the child's age) the incident is to be recorded in the ICT incident book and countersigned.
- Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content. No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.

All staff and adults in school should:

- Know who the Online Safety Lead and Designated Safeguarding Lead for Safeguarding is so that any misuse or incidents can be reported which involve a child.
- Be up-to-date with online safety knowledge appropriate for the age group and reinforce through the curriculum.
- Be familiar with the Positive and Restorative Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/Designated Safeguarding Lead immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Alert the Online Safety Lead of any new issues and risks that may need to be included within policies and procedures.
- Not use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account. The following content should not be created or accessed on ICT equipment at any time:
    - Pornography and "top-shelf" adult content
    - Material that gratuitously displays images of violence, injury or death
    - Material that is likely to lead to the harassment of others
    - Material that promotes intolerance or discrimination on grounds of race, sex, disability, sexual orientation, religion or age
    - Material relating to criminal activity, for example buying and selling illegal drugs
    - Material relating to any other unlawful activity e.g. breach of copyright
    - Material that may generate security risks and encourage computer misuse

(It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This will avoid problems later when monitoring systems are alerted to the content.)

- Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children should know what to do in the event of an incident.
- Report accidental access to inappropriate materials to the online safety Lead and or control this with the Local Control options via your broadband connection.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the SCC incident reporting procedure in the same way as for other non-physical assaults.

Mobile phone communication and instant messaging

- Staff are advised not to give their home or mobile telephone number to pupils or parents/carers. Mobile phone communication should be used sparingly and only when deemed necessary.
- Photographs and videos of pupils should not be taken with mobile phones.
- Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils' text messages other than for approved school business.
- Staff should only communicate electronically with pupils from school accounts on approved school business e.g. school work.
- Staff should not enter into instant messaging communications with pupils.
- Staff should not make or accept friend requests from pupils on any social media platforms.

Personal Use

In the course of normal operations, ICT resources are to be used for business purposes only. Staff who have been given the use of a school laptop or iPad and will be removing it from the premises will be expected to sign for its use on receipt. Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite. The school permits limited personal use of ICT facilities by authorised users. Staff may use school equipment for authorised business use under the following conditions:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.
- Personal use of the Internet must not involve attempting to access the categories of content described above.
- Passwords must be protected and account details must not be shared.

Using personal devices

- Personal data accessed by staff on their own devices must be kept secure in order to avoid a data breach and to remain compliant with GDPR. Access to personal data via staff email is permitted using a personal mobile device providing these are protected by fingerprint technology or 6 digit passcode lock.
- Personal data must not be saved onto personal mobile devices or any insecure public online file hosting and sharing services. Where access is required to school files, this must be via a staff laptop where protection is achieved through the Firewall and VPN (Virtual Private Network).
- Personal mobile devices used to access staff emails must not be shared with other family members or friends.

Working from home and securing personal data

- Personal data held in physical documents taken home by staff must be kept secure to avoid a data breach and to remain compliant with GDPR. As far as possible staff must keep data in an electronic format on a staff laptop or an encrypted memory device when working from home.
- Documents with minimal personal data such as pupil workbooks are low risk and can be taken home. Documents containing significant amounts of personal data such as pupil records and annual or termly reports require more scrutiny to ensure they are adequately protected.
- Any such documents should be kept in a closed folder, such as one with a zip lock and the folder should be labelled with the staff name and contact details in case of loss. Staff should ensure the documents are kept in a secure area of their house (ideally locked) and when returning the documents to school, be placed immediately back in their original storage place rather than left on

class desks or other insecure locations. The school should consider whether such documents should be signed in and out.

- If working from home for prolonged periods (due to COVID) staff should be especially mindful of protecting data by adopting the following practices;
  - Taking care to use BCC when emailing multiple recipients (for example class parents)
  - Caution should be exercised when participating in Zoom calls to parents and pupils. Please keep personal data to a minimum and ensure the appropriate parameters are set up for all participants. It is especially important to ensure parents cannot record the Zoom conversation. There is no definitive legislation on whether you can/cannot record your own conversations with parents, however if you do then **please obtain parental consent and explain how long the recording will be kept for and for what purpose, and who will access it.** Please note that a parent can request access to recordings made, via a Subject Access Request, therefore you must ensure you have a legitimate need to make any recordings.
  - Taking care not to delete information by accident or store in the wrong area (for example, on laptop desktops rather than school drives, cloud based systems or encrypted devices)
  - Taking particular care of the transportation of paper records as detailed above.

Children and Parents

Children are expected to use the internet and other technologies within school including downloading or printing of any materials in a responsible way as taught by the teachers. Each child receives a copy of the Acceptable Use Agreement on first-time entry to the school. This is read with the parent/carer, signed and returned to school. The agreements are there for children to understand what is expected of their behaviour and attitude when using the internet and other technology. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

It is hoped that parents/carers will explain and discuss the agreement with their child so that it is clearly understood and accepted. This is also intended to provide support and information to parents/carers when children may be using the Internet beyond school. We keep a record of the signed forms.

The school promotes a positive attitude to using the internet and we want parents to support their child's learning and understanding of how to use online technologies safely and responsibly. We do this by publicising e safety on the school website and by teaching children how to agree rules for use of the Internet.

Children should be:

- Involved in the review of Acceptable Use Agreement through School Council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Agreement whilst within school as agreed whenever a new child attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through the Computing curriculum, PSHE lessons or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

Consequences In the Event of Inappropriate Use

Should a child be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child's use for a particular lesson or activity.
- Further misuse of the agreement may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or is deemed to have misused technology against another child or adult.

In the event that a child **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The Curriculum and Tools for Learning

We teach children how to use the Internet safely and responsibly. They are also taught, through ICT/Computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies are taught by the time they leave the school.

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

These skills and competencies are taught within the national curriculum so that children have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school.
- Identifying information, e.g. I am number 8 in the school Football Team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded.

Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

Websites

The uploading of images to the school/ website should be subject to the same acceptable agreement as uploading to any personal online space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

Mobile Technology

Children are not permitted to have mobile phones or mobile devices in class or with them at break times.

If a child brings a mobile phone into school for communication at other time (e.g. on their way home) then it must be stored in a safe place by the class teacher and switched off.

Digital Images

Staff have access to cameras, iPads, web cams and scanners. There may be instances when staff use their own photographic equipment, to take a high quality image. These images must be stored to a central place e.g. – Teacher/photographs and films or Office / website within a few days. Images of children should be stored carefully in accordance with photo permission forms:

- as a record of significant events in the life of the school;
- to display and share in the school and educational communities;

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both. Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. It is current practice by external media such as local and national newspapers to include the full name of children in their publications. Photographs of children should only be used after permission has been given by a parent/carer.

Video-Conferencing and Webcams

The use of webcams to video-conference will be via a filtered service. Publicly accessible webcams are not used in school. Taking images via a webcam should follow the same procedures as taking images with a digital camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school. Children need to tell an adult immediately of any inappropriate use by another child or adult. (This will be part of the Acceptable Use Agreement).

Managing Social Networking and Other Web Technologies

The school does not promote use of social networking sites within the curriculum, we teach children about such uses of technology through online safety education.

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all staff but *is not recommended*. Owing to the public nature of such websites, it is advisable for staff and governors to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff and governors should not engage in personal online contact with students outside of authorised school systems.
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff and governors should not comment on issues relating to school, on any social networking site.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- Social networking is not used for communicating with students, even for professional purposes.
- Staff should not give out home or mobile telephone numbers or undertake instant messaging with pupils or parents.
- Our Home School Agreement states that *parents should not bring the name of the school, staff, parents or pupils into disrepute in public forums such as social networking sites (e.g. Facebook)*

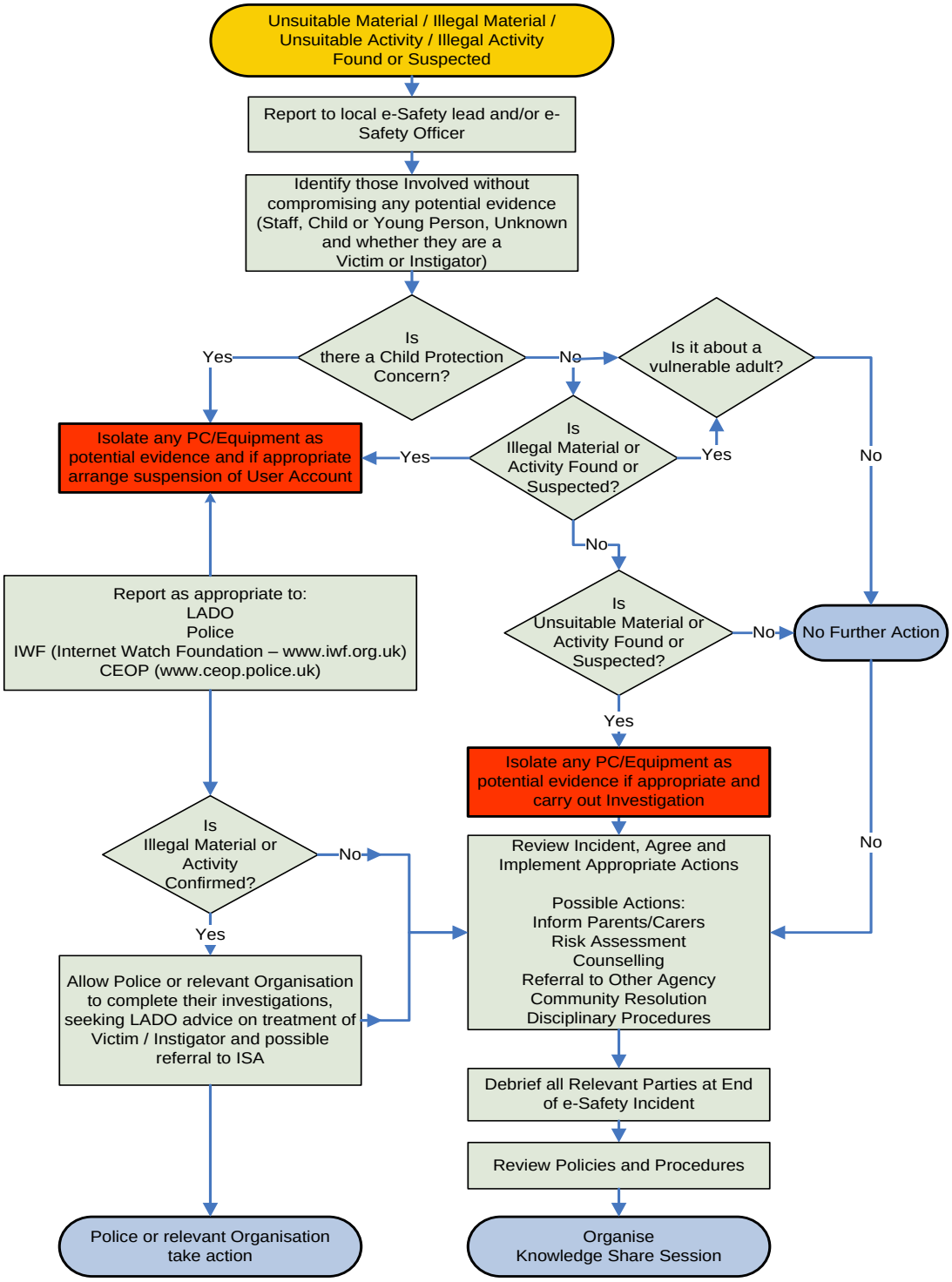
Filtering

Our broadband internet service has a filter system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. All filtering is controlled via Suffolk County Council. Local controls enable access to specific websites and provide the option to add to a 'restricted list'. Children are directed to use specific child friendly search engines (e.g. DuckDuckGo) and should only use a full search engine, e.g. Google, with adult supervision.

Links to Other Policies – Positive and Restorative Behaviour and Anti-Bullying Policies

Please refer to the Positive and Restorative Behaviour Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs. The Anti-bullying Policy refers to cyber bullying issues. All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT/Computing and PSHEE materials for children and their parents/carers. People should not treat online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children and adults.

Fig 1: Online Safety Flow Chart



Acceptable Use of ICT Agreement for Staff, Governors, Volunteers and Visitors

This agreement applies to all online use, mobile communications and anything downloaded or printed. The online safety policy is available in school to refer to about all issues and procedures.

All adults within the school must be aware of their safeguarding responsibilities when using technologies and they are asked to sign this agreement. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- In case of a data breach of personal data I will report this to the Data Protection Officer and Headteacher within the required 72 hours.
- I know that I must only use the school equipment in an appropriate manner and professional manner
- I understand that I need to give permission to children before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the internet.
- I will report accidental misuse.
- I will report any incidents of concern for a child's safety to the Designated Safeguarding Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Safeguarding Lead is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones for educational purposes.
- I know that I should complete virus checks on my laptop, memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the current Data Protection legislation and have checked I know what this involves.
- I know how to keep myself and other people safe and how to protect personal and sensitive data when working from home.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights and I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I will follow the schools guidance on the use of personal mobile phones and other devices.
- I will not use social networking sites to discuss school related issues.

I have read and understood the online safety policy and the Acceptable Use Agreement and know that by following them I have a better understanding of online safety and my responsibilities to safeguard children when using online and mobile technologies.

Signed……Date……

Name (printed)…… Role……

Acceptable Use of Computing/ICT - Agreement for Children – Key Stage 2

Computing/Information Communication Technology (ICT) including the internet, email and mobile technology has become an important part of learning in every school. At Hundon and Thurlow Primary Federation we use a filtered internet and secure school email system but we expect all children to be safe and responsible users. Teachers explain the rules below to their class but please also read and discuss these with your child and return the slip at the bottom of this page. Children use Computing/ICT to varying degrees as they progress through the school, according to their age group and the objectives in the National Curriculum. This agreement covers use through your child's time in school and may be updated as technology develops and changes.

My online safety agreement

- I will look after myself and others by using the internet in a safe and responsible way and only use school ICT for school purposes
- I will only open my own school files
- I will not bring any memory sticks or other storage devices into school
- I will only use the internet with adult permission and only for school learning
- I will only email, open email attachments, chat or message people that a trusted adult has approved as part of my lesson
- I will only send messages that are polite and friendly
- I agree never to fill out forms or give out passwords or personal information like my full name, address or phone numbers
- I agree never to post photographs or video clips without permission and I will not include my name with any photographs
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to an adult
- I know what to do if I see anything on the internet that makes me feel uncomfortable and I will tell an adult immediately
- I will not use or download apps without permission
- I understand that the school may check my computer files and may monitor any internet sites I visit
- I know I should follow these guidelines as part of the agreement with my parent/carer
- I know that if I break these rules I may not be allowed to use school computing equipment

Acceptable Use Agreement for Children – reply slip

We have discussed this agreement and …… (name) in …… agrees to follow these rules and support the safe use of Computing/ICT at Hundon and Thurlow Primary Federation

Parent/Carer signature …… Date ……