St. Andrew's CEVA Primary School
Acceptable Internet Use Policy

This policy has been adapted from the Northamptonshire Acceptable Use Policy which was designed for use by Headteachers, Governors, e-Safety Leaders and the Designated Person for Child Protection. This Policy should be used in conjunction with the Child Protection Policy, the Health and Safety Policy, the AntiBullying Policy and the ICT curriculum policy. This policy was originally drafted by N.C.C. as a guide for all schools and educational settings, where many Esafety risks and management issues are the same, with the same key messages for children, young people, their parents/carers and staff/other users.

The content has been adapted to the needs and curriculum of our children and young people whilst still reflecting the key messages and procedures required to successfully implement the N.C.C. requirements. This policy has been developed by the Children and Young People's Service in consultation with Education Welfare - CYPS, Northamptonshire Police, the Local Safeguarding Children's Board Northamptonshire, Governors and Parents/Carers and Children.

1. What is an AUP (Acceptable Use Policy)?

St. Andrew's CEVA Primary follows guidance from the LA contained within this policy. An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all on-line technologies (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, mobile phones and games) to safeguard adults and children and young people within the school setting. It details how the school will provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies, beyond the school setting. It also explains procedures for any unacceptable or misuse of these technologies by adults or children and young people.

2. Why have an AUP?

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst St. Andrew's CEVA Primary School acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

As part of the Every Child Matters agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected

from potential harm both within and beyond the school environment. Therefore, the involvement of children and young people and parent/carers is also vital to the successful use of on-line technologies, so this policy also aims to inform how parents/carers and children or young people are part of the procedures and how children and young people are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

3. Aims

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone.
- To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

4. Policy Statements

4.1 Education –Pupils

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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people will 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, social media sites and e-mailed to other people does not include any personal information including:

- 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 Youth Football Team

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE and should be regularly revisited. We use the Rising Stars Scheme of Work, Switched on ICT, to teach Internet and E-mail lessons from Years 1 to 6, where each unit of work contains

guidance on e-safety and we use the www.thinkuknow.co.uk resources for KS1 and KS2 for explicit teaching. All children complete an e-safety unit in the Autumn Term.

- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be 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. *Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.*
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

4.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

4.3 Education – Staff

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out. Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff (https://boost.swgfl.org.uk/)
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy E-Safety Policy and Acceptable Use Agreements. Online Safety BOOST includes an array of presentations and resources that can be presented to new staff (https://boost.swgfl.org.uk/)
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Leader will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E- Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Leader will provide advice / guidance / training to individuals as required. Online Safety BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff (https://boost.swgfl.org.uk/) It includes presenter notes to make it easy to confidently cascade to all staff.

5. Roles and responsibilities of the school:

5.1 Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated an Online Safety Leader (subject co-ordinator) to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- The Headteacher / Principal 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 Leader.
- The Headteacher and (at least) another member of the Senior Leadership Team 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 a later section – "Responding to incidents of misuse" and relevant Local Authority HR).
- The Headteacher is responsible for ensuring that the Online Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Time and resources will be provided for the Online Safety Leader and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the Governors at the Learning Provision meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors will be made aware of e-Safety developments from the Learning Provision meetings.
- The Governors **MUST** ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An e-Safety Governor (can be the ICT or Child Protection Governor) will challenge the school about having an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:
    - Challenging the school about having:
        - Firewalls
        - Anti-virus and anti-spyware software
        - Filters
        - Using an accredited ISP (Internet Service Provider)
        - Awareness of wireless technology issues
        - A clear policy on using personal devices.

5.2 Online Safety Leader

It is the role of the designated Online Safety Leader to:

- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-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 and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform.

- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Child Protection and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found later in this document).
- Reports regularly to Senior Leadership Team.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Work alongside the ICT Technician, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.

5.3 Network Manager / Technical staff:

The Network Manager / 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 / other relevant body 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 policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher /Senior Leaders / Online Safety Leader for investigation / action / sanction.
- That monitoring software / systems are implemented and updated.

5.4 Designated Safeguarding Person

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

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

5.5 Staff or Adults

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the Designated Person for Child Protection is within school or other setting so that any misuse or incidents can be reported which involve a child.
- They have an up to date awareness of online safety matters and of the current school / academy Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).

- They report any suspected misuse or problem to the Headteacher / Senior Leader Team/ Online Safety Leader for investigation / action / sanction.
- 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.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities 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 and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Ensure that children and young people are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the Online Safety Leader in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick (encrypted) or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.

5.6 Children and Young People

Children and young people:

- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Taught to use the Internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Issued with a certificate of e-safety at the start of every year to demonstrate they have completed an e-safety age appropriate refresher course.

6. Acceptable Use Rules

Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables 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.

We want our parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, the rules

are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.
Further to this, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.*

Each child or young person will receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.
School will keep a record of the signed forms.

7. Inappropriate Use

7.1 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)
Should a child or young person be found to misuse the on-line facilities whilst at school the following consequences will occur:

- Any child found to be misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules will 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 will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

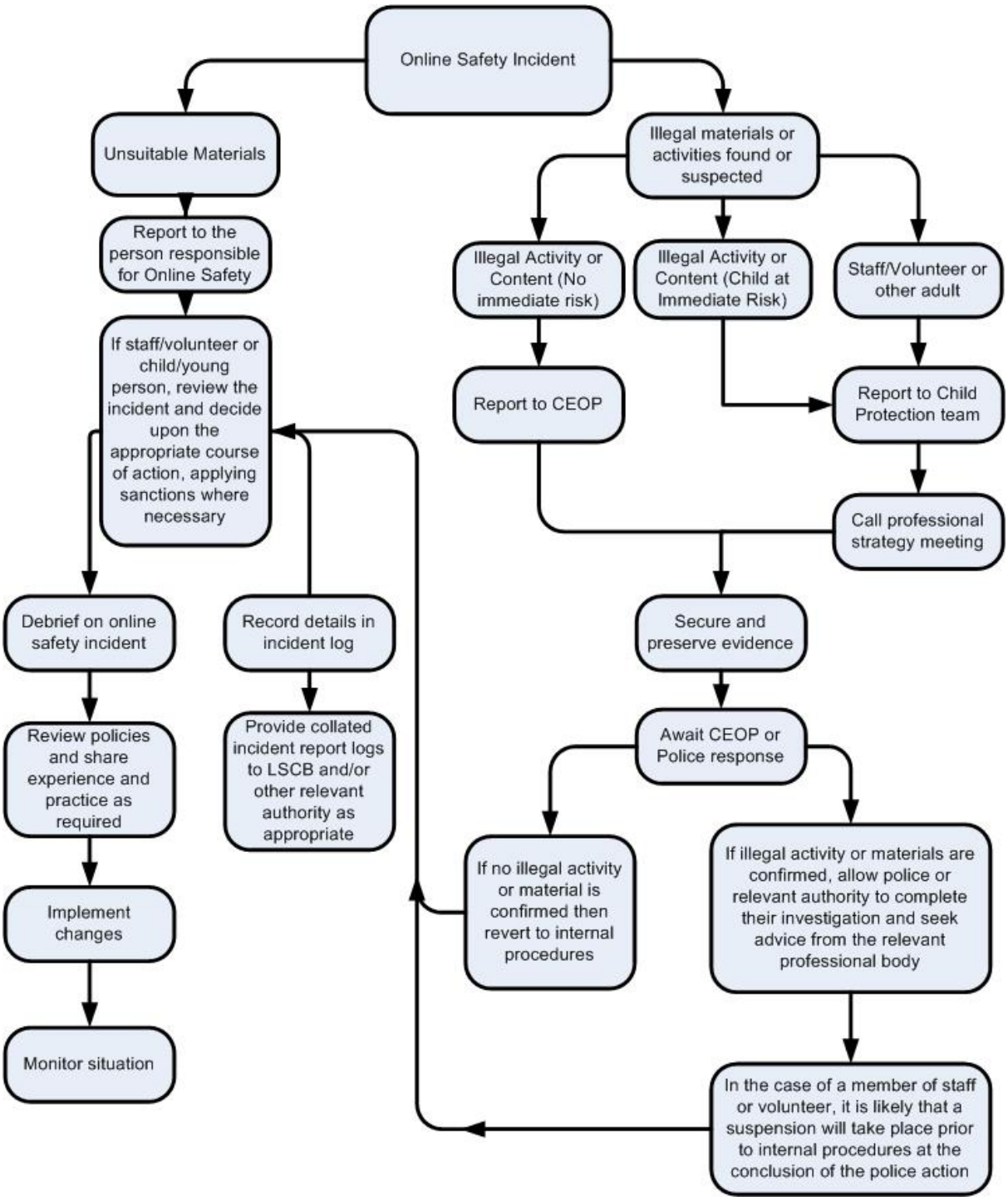
In the event that a child or young person **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person 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.

Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

* For a list of the Copyright Licences go to: https://www.gov.uk/guidance/copyright-licences-information-for-schools

7.2 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, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

7.3 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 should be followed:

- Have more than one senior member of staff / volunteer involved in this 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 (to provide further protection).
- 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 (except in the case of images of child sexual abuse – see below)
- 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 by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances 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
    - 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.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

8. Links to other policies

8.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. 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 and PSHE materials for children and young people and their parents/carers. People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour.

8.2 Allegation Procedures and the Child Protection Policy
Please refer to the Allegation Procedure in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Headteacher immediately or Chair of Governors in the event of the allegation made about the Headteacher.

The DfE White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people and young people about homework or any other school issues either in or beyond school and any such action should be dealt with. We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.

Please refer to the Child Protection Policy the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

8.3 PSHE
We link the teaching and learning of e-Safety with our PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people.

8.4 Disciplinary Procedure for All School Based Staff
In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Reviewed: September 2020
Signed: A Jones
Date of next review: September 2021

Appendix 1

Staff Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school / academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I

will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to 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 will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school / academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to

Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name: .....

Signed: .....

Date: .....

Appendix 2

Pupil Acceptable Use Policy Agreement

Foundation stage/ Key Stage 1

This is how we stay safe when we use computers:

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

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Appendix 2

Acceptable Use Policy Agreement

Key Stage 2

This is how we stay safe when we use computers:

I understand that while I am a member of St Andrew's CEVA Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.
- I understand that my use of the internet will be monitored.
- I will keep my password safe and will not use anyone else's (even with their permission).
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal ICT equipment if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows.
- We know that we can go to www.thinkuknow.co.uk for help.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

Child Agreement:

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, , website etc.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Appendix 3
Further Information and Guidance

The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)

Appendix 4

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....
.....

Details of first reviewing person

Name: .....
Position: .....
Signature: .....

Details of second reviewing person

Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken
