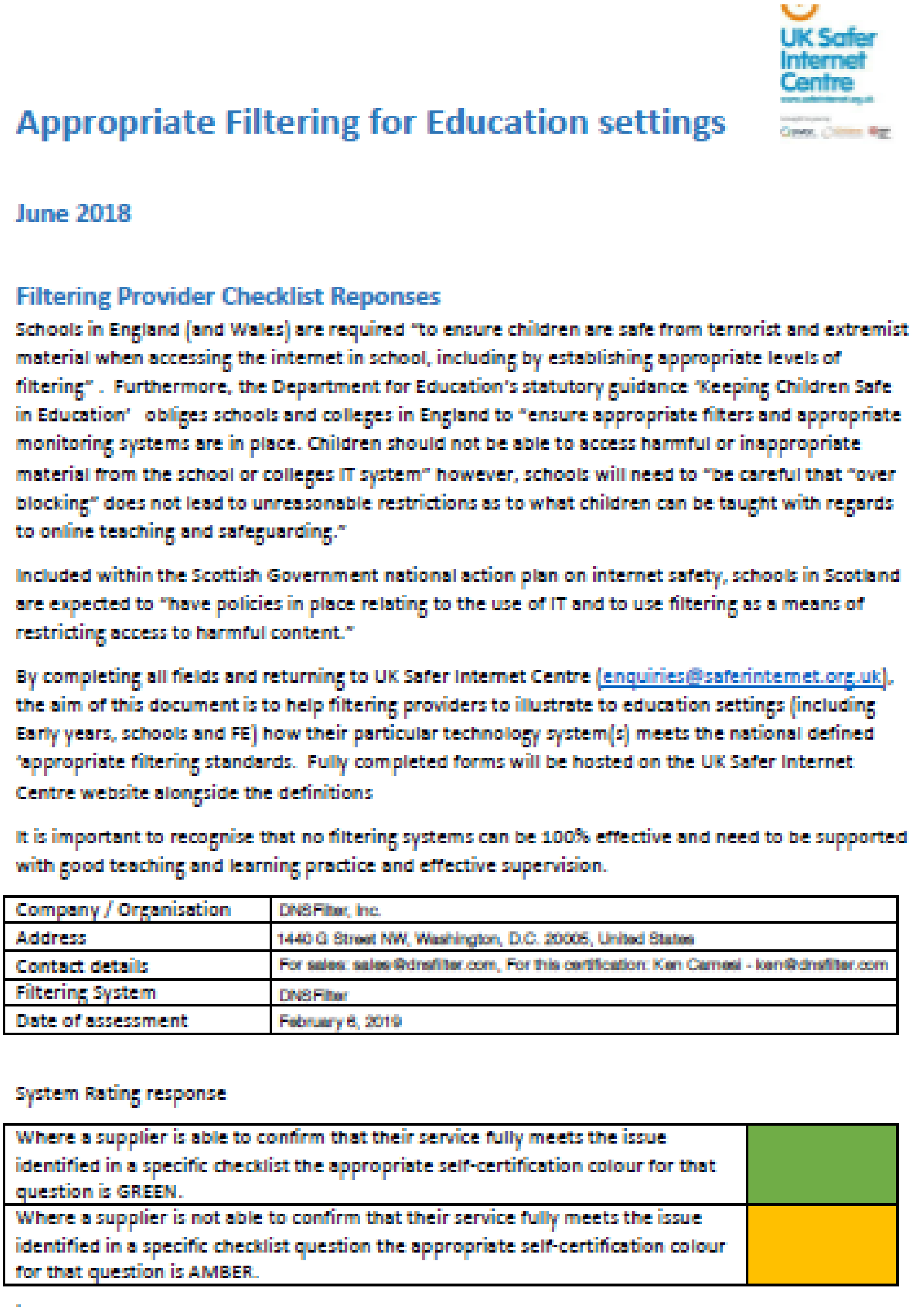
Appendix 1 – Appropriate Filtering for Education Setting



Appropriate Filtering for Education settings

June 2018

Filtering Provider Checklist Reponses

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" . Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

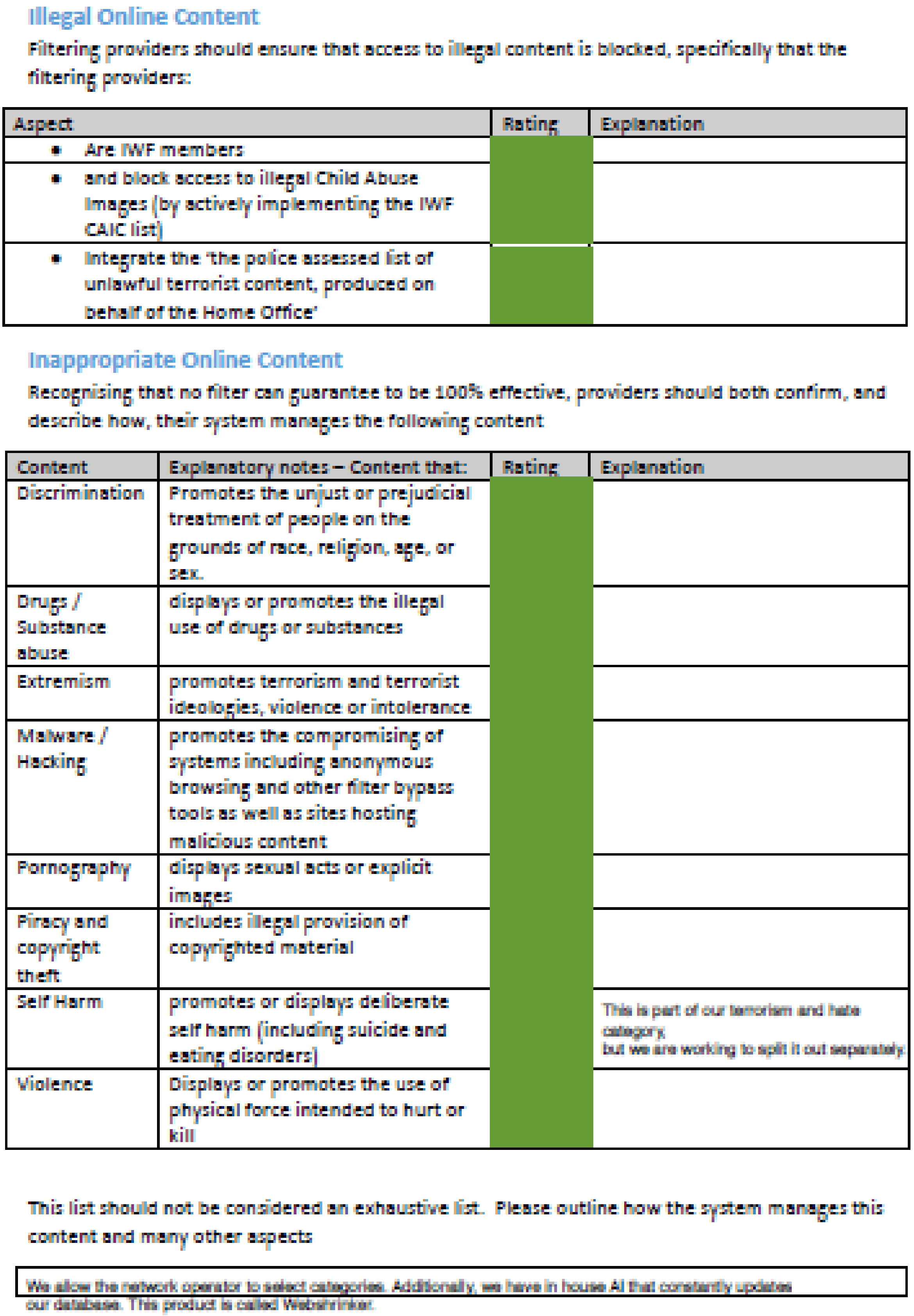
It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	DNSFilter, Inc.
Address	1440 G Street NW, Washington, D.C. 20005, United States
Contact details	For sales: sales@dnsfilter.com, For this certification: Ken Carnesi - ken@dnsfilter.com
Filtering System	DNSFilter
Date of assessment	February 6, 2019

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟨

-



Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members	🟩	
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)	🟩	
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	

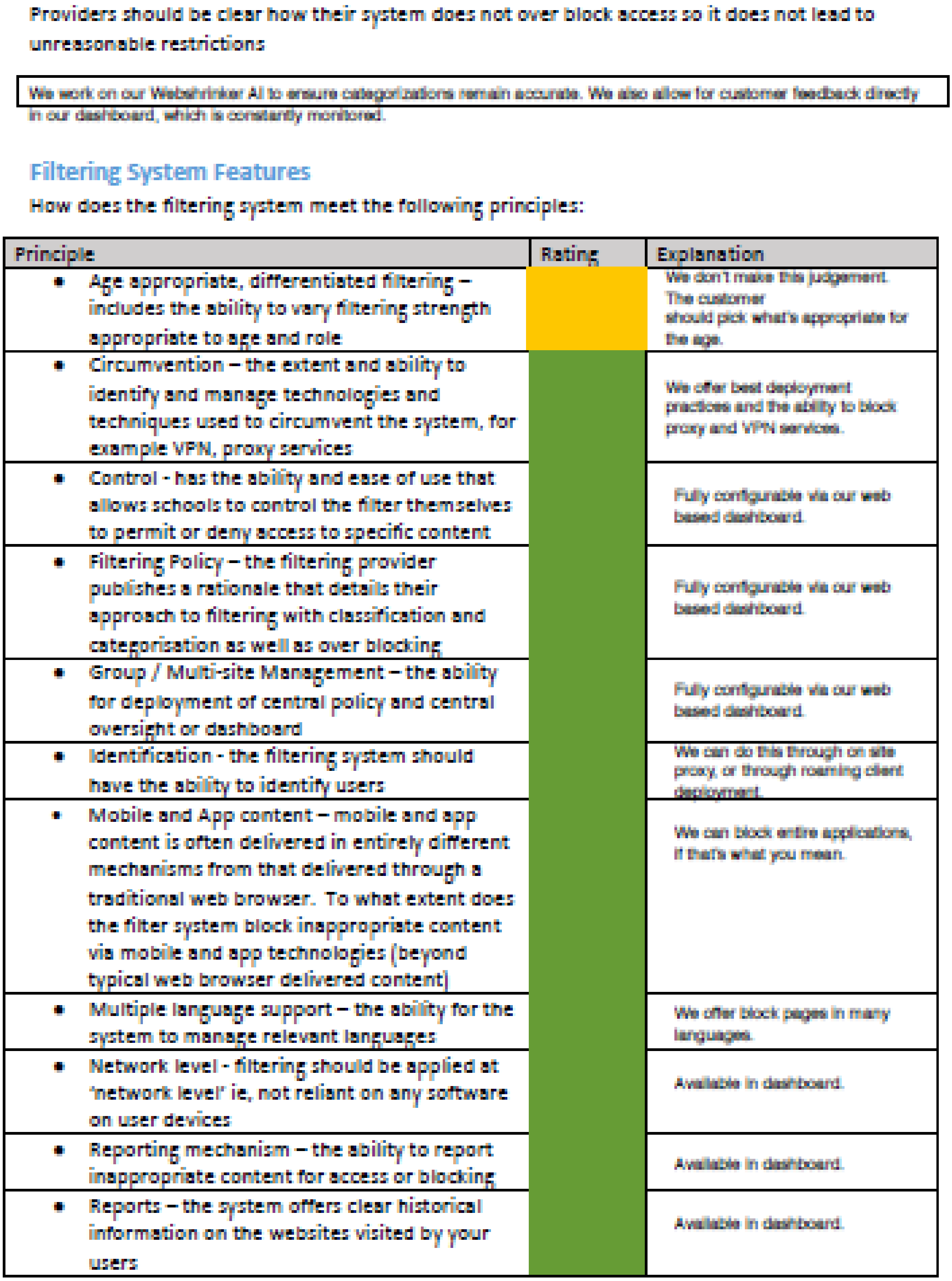
Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.	🟩	
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	
Pornography	displays sexual acts or explicit images	🟩	
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	This is part of our terrorism and hate category, but we are working to split it out separately.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

We allow the network operator to select categories. Additionally, we have in house AI that constantly updates our database. This product is called Webshrinker.



Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

We work on our Webshrinker AI to ensure categorizations remain accurate. We also allow for customer feedback directly in our dashboard, which is constantly monitored.

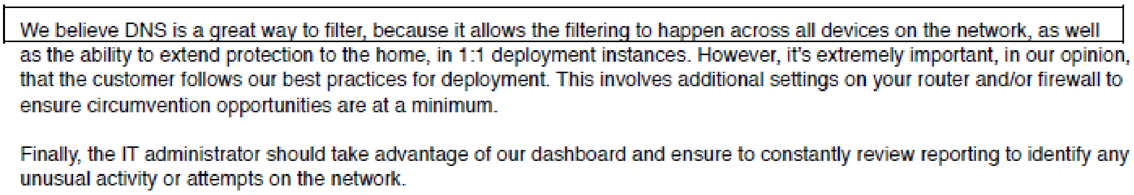
Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role	🟨	We don't make this judgement. The customer should pick what's appropriate for the age.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services	🟩	We offer best deployment practices and the ability to block proxy and VPN services.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	🟩	Fully configurable via our web based dashboard.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Fully configurable via our web based dashboard.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Fully configurable via our web based dashboard.
• Identification - the filtering system should have the ability to identify users	🟩	We can do this through on site proxy, or through roaming client deployment.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)	🟩	We can block entire applications, if that's what you mean.
• Multiple language support – the ability for the system to manage relevant languages	🟩	We offer block pages in many languages.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices	🟩	Available in dashboard.
• Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Available in dashboard.
• Reports – the system offers clear historical information on the websites visited by your users	🟩	Available in dashboard.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard



We believe DNS is a great way to filter, because it allows the filtering to happen across all devices on the network, as well as the ability to extend protection to the home, in 1:1 deployment instances. However, it's extremely important, in our opinion, that the customer follows our best practices for deployment. This involves additional settings on your router and/or firewall to ensure circumvention opportunities are at a minimum.

Finally, the IT administrator should take advantage of our dashboard and ensure to constantly review reporting to identify any unusual activity or attempts on the network.

Provider Self-Certification Declaration

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Kenneth B. Carnesi, Jr.
Position	CEO
Date	February 6, 2019
Signature	

Appendix 2

Acceptable Use Agreement / Code of Conduct - Staff and Governors

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school Computing systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of Computing in their everyday work.

The school will try to ensure that staff and volunteers will have good access to Computing to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users. This policy links to our Social Networking and use of social media policy.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the Computing systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school Computing systems (eg 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 Computing 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 Computing 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 (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online 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 / 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school 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 Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or student 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 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:

- I understand that this Acceptable Use Policy applies not only to my work and use of school Computing equipment in school, but also applies to my use of school Computing 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.
- 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 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 computing 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 / Volunteer Name

Signed

Date

Appendix 3

Acceptable Usage Policy – Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school’s digital technologies will be responsible users and stay safe while using these systems and devices
- that school’s systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

This policy links to our Social Networking and use of social media policy.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored

- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.

- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- I will not access, copy, remove or otherwise alter any other user’s files, without permission.

- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, without permission from the school.

- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- 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).

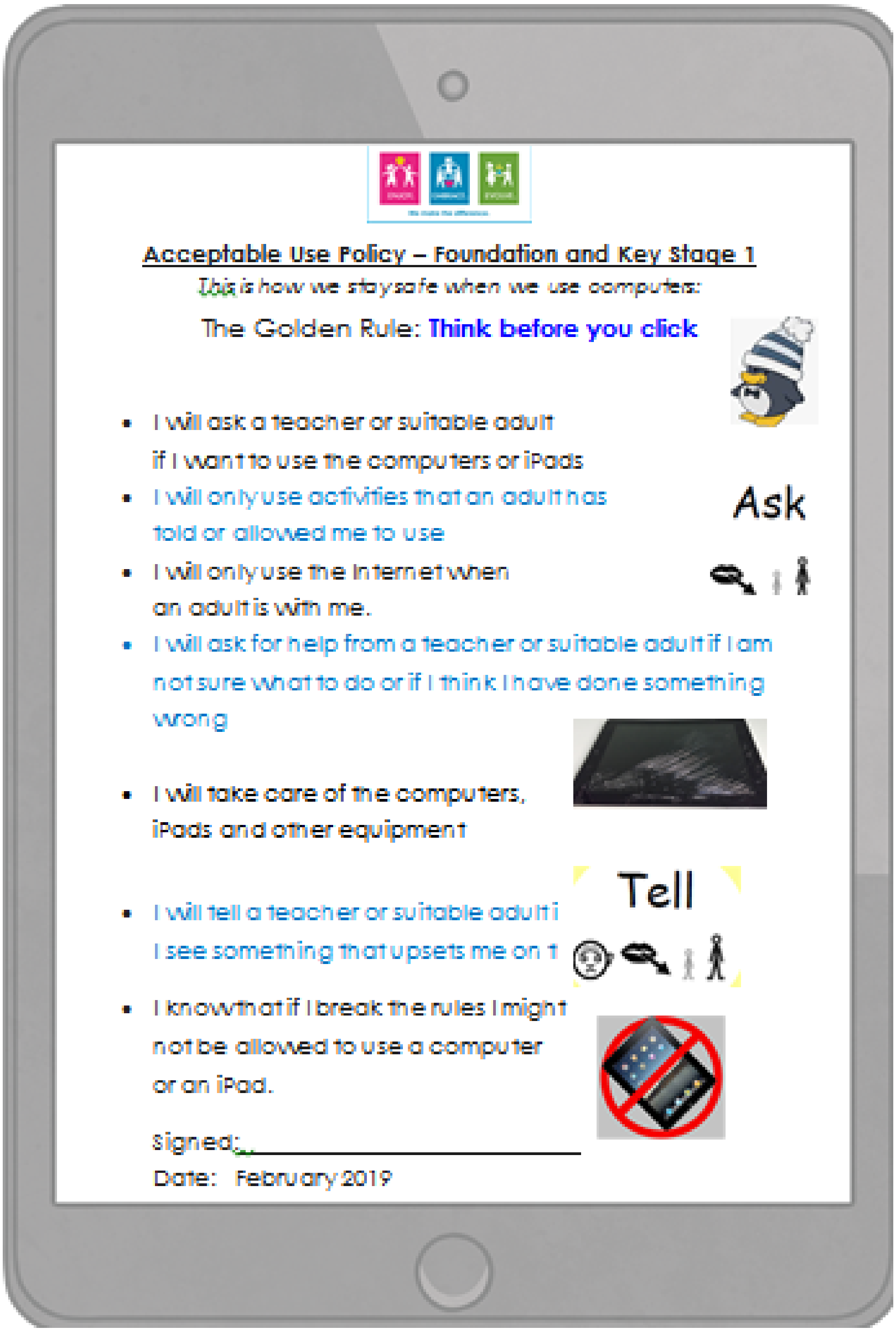
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school computing 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.

Name

Signed Date

Appendix 4 – Acceptable Use Policy Key Stage 1 and Foundation Stage



Acceptable Use Policy – Foundation and Key Stage 1

This is how we stay safe when we use computers:

The Golden Rule: **Think before you click**

- I will ask a teacher or suitable adult if I want to use the computers or iPads
- I will only use activities that an adult has told or allowed me to use

Ask

- I will only use the Internet when an adult is with me.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will take care of the computers, iPads and other equipment

Tell

- I will tell a teacher or suitable adult i I see something that upsets me on t
- I know that if I break the rules I might not be allowed to use a computer or an iPad.

Signed:______________________________

Date: February 2019

Appendix 5

Acceptable Usage KS2 Children –

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users

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.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, etc)
- I will not meet people offline that I have communicated with 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 act as I expect others to act toward me:

- 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 use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me:

- I will not use my own personal devices in school
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites in school.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, it will be dealt with by following our behaviour policy. This would include contact with parents and in the event of illegal activities involvement of the police

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

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 eg. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Class	
Signed	
Date	February 2019

Appendix 6

Acceptable Use Policy - Parents

This Acceptable Use Policy is intended to ensure:

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

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

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

Permission Form

Parent / Carers Name:________________________
Student / Pupil Name: ________________________ Class:____________________

- As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school.
- I know that my son / daughter has signed an **Acceptable Use Agreement** and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and Computing systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the Computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

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

Signed □ Date □

Appendix 7 – Online Safety Recording Log

Delph Side Primary School Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded in the Incident Log. This incident log will be monitored termly by the Head teacher. (to be used if CPOMS not available)

Online Safety Incident Log

Name of child:_______________________________

Date:

Reported by:

Room and computer / device __________________________________

Details of incident (incl evidence) Signed:________________________

Actions and Reasons

Signed:(DSL)______________________________ Date:______________________

Appendix 8 – Roles and Responsibilites

Role	Responsibility
Governors	Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body / Board has taken on the role of Online Safety Governor The role of the Online Safety Governor / Director will include: • regular meetings with the Online Safety Leader • attendance at Online Safety Group meetings • regular monitoring of online safety incident logs • regular monitoring of filtering / change control logs • reporting to relevant Governors / Board / Committee / meeting
Headteacher and Senior Leaders	*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 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 – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).* • *The Headteacher and Senior Leaders 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.* • *The Headteacher / 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.* • *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer / Lead.*
Online Safety Lead	• leads the Online Safety Group • 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. • provides training and advice for staff • liaises with school technical staff • receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (• meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs • attends relevant meetings of *Governors* • reports regularly to Senior Leadership Team
Designated Safeguarding Lead	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 • online-bullying
Teaching and Support Staff	• Are responsible for ensuring that: • they have an up to date awareness of online safety matters and of the current 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 ; Online Safety Lead* (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 • students / pupils understand and follow the Online Safety Policy and acceptable use policies • students / 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 lessons and other school activities (where allowed) and implement current policies with regard to these devices • *in lessons where internet use is pre-planned students / 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*

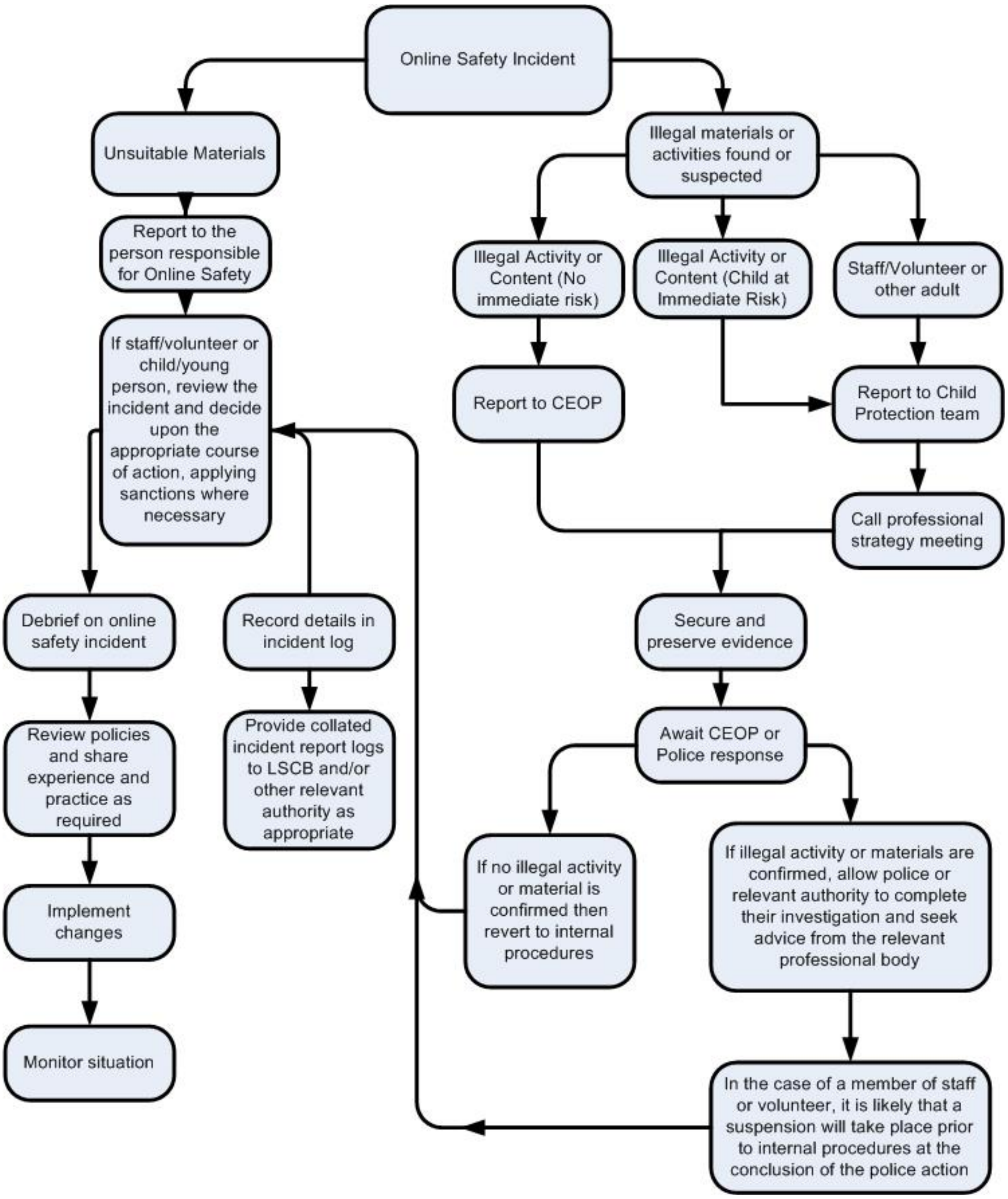
	searches
Students / Pupils	• are responsible for using the *school* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying. • should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's / academy's* Online Safety Policy covers their actions out of school, if related to their membership of the schoo
Parents and carers	Parents / 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, website, Facebook and See Saw Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events • their children's personal devices in the school
Online Safety Group	Members of the Online Safety Group will assist the Online Safety Officer / Lead (or other relevant person, as above) with: • the production / review / monitoring of the school Online Safety Policy / documents. • mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression • monitoring network / internet / incident logs • consulting stakeholders – including parents / carers and the students / pupils about the online safety provision • monitoring improvement actions identified through use of the 360 degree safe self-review tool
Technical Support Provider	The Network Manager / Technical Staff Computing is 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 Guidance that may apply.

	• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed • 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction • that monitoring software / systems are implemented and updated as agreed in school / academy policies .
Community Users	Community Users who access school systems as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school

Appendix 9 Monitoring of Online Safety Incidents

Online Safety Incidents Reporting Log **Delph Side Primary School**						
Date	***Time***	***Incident***	***Action Taken***		***Incident Reported By***	***Signature***
			What?	***By Whom?***		

Appendix 10 – Responding to incidents of misuse flowchart


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

Appendix 11 – Record of reviewing devices

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

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/ipad used for review (for web sites)

....

....

Web site(s) address / device	*Reason for concern*

Conclusion and Action proposed or taken

Appendix 12 – Online Safety Groups Terms of Reference

Purpose

To provide a consultative group that has wide representation from the Delph Side community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include

SLT member / Online safety coordinator	Designated Safeguarding Lead	Teaching staff member
Support staff member	Governor	Parent / Carer
ICT Technical Support staff	Pupils	

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held termly during the school day. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following

- To keep up to date with new developments in the area of Online Safety
- To (at least) annually review and develop the Online Safety Policy in line with new technologies and incidents
- To monitor the delivery and impact of the Online Safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training (pupils not to be present)
- To discuss training needs, including staff, parent/community awareness.
- To raise new community initiatives in response to training needs or as a result of polls/surveys
- To coordinate annual events such as Anti-Bullying Week or Safer Internet Day

Amendments

The terms of reference shall be reviewed annually from the date of approval.
They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Delph Side Primary School have been agreed
Signed by (SLT): Jonathan Fyne

ENJOY. EMBRACE. EVOLVE.
We make the difference.

Online Safety Policy
June 2019

Date: January 2018
Date for review: January 2019

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council

Appendix 13 - Notes on the legal framework

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an Online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Appendix 14 – Links to other organisations and documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring
Somerset - Questions for Technical Support
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom –Media Literacy Research

Online Safety Policy Appendices
June 2019