Diocese of Sheffield Academies Trust

Pye Bank CE Primary School

Online Safety and Acceptable Use Policy

Approved by:	Policy Review Committee	**Date:**	8th November 2021
Last reviewed on:	Sept 2021		
Next review due by:	Nov 2022		

Contents

Contents

Appendices:

Policy Introduction

Our school aims to:

1. Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
2. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
3. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Rationale

The children in today’s society have the opportunity to access a wide range of new technologies including the internet, a variety of communication technologies and other digital media. Online Safety encompasses both Internet technologies and electronic communications such as ipads, tablets and mobile phones. These are powerful and innovative tools which bring new opportunities for both teachers to teach and pupils to learn. Using such technologies promotes discussion, thinking, creativity, can stimulate learning and even raise educational standards and achievement. However, in order to use these technologies effectively, we need to educate our children about the benefits and risks they may encounter whilst online.

The 4 key categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

This Online Safety policy will be used in conjunction with other policies already embedded in school including the Behaviour, Anti-bullying, Safeguarding and Child Protection Policies. It is impossible to remove all risk. However, we will endeavour to build our pupils resilience to the risks they may encounter when online, so that they have the confidence and skills to stay safe.

Legislation and Guidance

This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2021, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Monitoring and Communication

The school will monitor the impact of the policy using:

- Monitoring of pupil activity during lesson times
- Logs of reported incidents
- Our parents and pupils views regarding online safety, whether through school council, questionnaires or workshops.

Communication of this Policy

1. All amendments will be published and where appropriate awareness sessions will be held.
2. Any Online safety updates will be included in the curriculum to ensure pupils are aware.
3. Online safety training will be established across the school to include a regular review of updates within this policy.
4. The key messages contained within the Online Safety Policy will be reflected and consistent within all acceptable use policies in place within school.
5. We endeavour to embed online safety messages across the curriculum whenever the internet or related technologies are used.
6. Incidents will be dealt with, whether in or out of school in accordance with this policy, and other policies including Behaviour, Anti-bullying and Safeguarding. The school will, where known, inform parents of any incident which demonstrates inappropriate online safety behaviour.

Senior Leadership

- The senior leadership team are responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school Online Safety policy and the use of any new technology within school.
- The Online Safety policy will be accessible to and discussed with all members of staff.

Staff

- The Staff Acceptable Use Policy Agreement will be discussed and signed.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Pupils

- Pupils together with their parent(s) need to read and agree to the Acceptable Use Agreement for Internet use in school. Parents need to approach the school if they disagree with any parts of the agreement.

- Online Safety posters will be prominently displayed around the school.
- Teachers will reinforce the Pupil Acceptable Use Agreements through ICT lessons and will use the SMART rules within the curriculum.

Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school online community.
- A Parents update at one coffee morning each year will be offered to highlight the dangers and provide useful information on how children can stay safe when using the internet.

Roles and Responsibilities

We believe that Online Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

The following responsibilities demonstrate how each member of the community will contribute.

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix G)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix H) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a regular full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix H) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying and online peer on peer abuse are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix G), and ensuring that pupils follow the school's terms on acceptable use (appendices E and F)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix H) and dealt with appropriately in line with this policy
- Ensuring that any incidents of online peer on peer abuse and cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices E and F)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix G).

Educating and Training School Members

Pupils

Pupils will be taught about online safety as part of the curriculum: The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

All Staff and Governors

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including online peer on peer abuse, cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

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 and in promoting the positive use of the internet and social media. The school will take every opportunity to help parents understand these issues through:

1. Parents' evenings and Coffee Morning
2. Newsletters
3. Letters
4. Online communication (Class Dojo, the school website)

Cyber-Bullying

Definition of Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

Pupils are not allowed to have electronic devises in school or on school trips. However, on occasion, the following may apply.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Using Digital and Video Images (see appendix I)

All members of the school community need to be aware of the risks associated with the sharing and posting of digital images on the Internet. The images used cannot be removed from the internet and so are there forever.
This could be damaging and cause harm or embarrassment to individuals whether now or in the future years. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.
Therefore it is important that we as educators take the following actions:

- Teach our members the risks associated with the taking, sharing and distribution of images. For example, on social networking sites, they are on view to potential employers (cyber vetting) and potential groomers. We need to teach all school members about their digital footprint and the risks attached with publishing their own images.
- Staff to plan the photographs they take for educational purposes and ensure pupils are appropriately dressed. We need to ensure we have parental consent to use or publish those images. Images should only be taken on school equipment, use of personal equipment needs to be authorised by the head teacher.
- Learners are taught not to upload, share or distribute images of themselves or others to the internet without seeking permission. Educational Videos like "Think Before You Post" (by CEOP) will be viewed to get this message across.
- Students‟ / Pupils‟ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website, prospectus etc.

Managing Internet Access and Security

Pupils will continue to use the Internet outside school and so will need to learn how to evaluate Internet information and that they need to take a responsibility of their online safety, behaviour and security. As a school it is our role to ensure pupils can balance the benefits of using the internet with an awareness of the potential risks.

ICT System Security

1. Users need to seek advice and permission from the school technical team before downloading any programs. An administration code is required.
2. The school ICT systems capacity and security will be reviewed regularly by the schools ICT technical team.
3. Virus protection is installed and updated regularly by the school technical team on all workstations within the infrastructure.

Content Filtering

1. The school works in partnership with Smoothwall to ensure filtering systems are as effective as possible.
2. The school's internet provision includes filtering appropriate to the age and maturity of our pupils.

3. The school will always be proactive regarding the nature of content which can be viewed through the school’s internet provision.
4. The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy.
5. If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety Coordinator. All incidents should be documented.
6. If users discover a website with potentially illegal content, this should be reported immediately to the online safety Coordinator. The school will report such incidents to appropriate agencies including the filtering provider.
7. The school will regularly review the filtering product for its effectiveness.
8. Any amendments to the school filtering or block-and-allow lists will be checked and assessed prior to being released or blocked through the school’s technician, Online Safety coordinator or YHGfL
9. Pupils will be taught to assess content as their internet usage skills develop.
10. Levels of internet access and supervision within our school may well vary depending on the user. Pupils and Teachers may have different filtering policies applied to their internet use, either temporarily or permanently as we have moved towards a less locked down service.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of *Internet access.*

Setting Passwords

1. A secure username and password convention exists for all system access. The technicians can access all equipment including resetting users’ passwords when necessary.
2. Key Stage 1 pupils will have a generic pupil logon to all school ICT equipment.
3. Pupils at Key Stage 2 are moving towards individually-named user account and password for access to ICT equipment.
4. All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
5. Users should change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
6. All staff and pupils have a responsibility for the security of their username and password. ***Users must not allow other users to access the systems using their log on details*** and must immediately report any suspicion or evidence that there has been a breach of security.
7. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. All personal passwords that have been disclosed should be changed as soon as possible.
8. Never save system-based usernames and passwords within an internet browser.
9. All access to school information assets will be controlled via username and password.
10. No user should be able to access another user’s files unless delegated permission has been granted.
11. Users should create different passwords for different accounts and applications.
12. Users should use 8 characters including numbers, letters and special characters in their passwords (! @ # $ % *)

Internet Access

1. Pupils and Staff will discuss and sign the Acceptable Use Policy to know what Internet use is acceptable.
2. When a member of the school community departs from the school the technical team must ensure any user information held by this member has been deleted to safe guard children and

school data. This includes google accounts, remote access, subscription accounts or access to school information sites such as ROL etc .

3. Any visitors who are with the school for a period of time must also agree to the Acceptable Use Policy relevant to them.
4. Parents will be informed that pupils will be provided with supervised Internet access and will be asked to read the Acceptable Use Policy with their child. If they disagree it is the parent's responsibility to inform the school. (This information will be included in all new pupils starter packs)

Internet Use

1. Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
2. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
3. School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
4. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Handling Incidents – See Response to an Incident of Concern in Appendix B

1. Internet misuse will be dealt with and sanctions given by the class teacher at the time of the misuse.
2. Incidents will be reported to the Online safety Coordinator/ Child Protection Liaison Teacher, / The Head Teacher who will judge whether it is necessary to just log the incident, or inform the Sheffield Safeguarding Team or/and the police.
3. If misuse is repeated, Parents will be informed.
4. Any complaint about staff misuse will be referred immediately to the Head Teacher and discussions with the local police if appropriate.
5. Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
6. Illegal issues with be handled through discussions with the Head Teacher, Child Protection Liaison Teacher, Governor Representative and Local Police.

Emailing

1. Pupils/staff must immediately tell a teacher/head teacher if they receive offensive or any unknown external e-mail within their own or group accounts.
2. Pupils must not reveal personal details of themselves (including their e-mail address) or give information of other peoples details in e-mail communication, or arrange to meet anyone without specific permission.
3. Any e-mail in school should only be sent through approved email accounts setup by the class teacher.
4. Pupils must have permission before emailing in school. The passwords on these accounts can be changed by the teacher after the session if so required.
5. Staff must only use the school email system for work purposes. Staff should not use personal emails for work purposes.

Social Networking Sites

Pupils

1. The School uses Smoothwall which blocks/filters access to social media sites unless a specific use is approved as in Twitter and facebook for school sites only.
2. Pupils are advised to only use moderated sites specifically for their age group and to seek consent from an adult.

3. Pupils are advised never to give out personal details or complete online forms of any kind which may identify them or their location
4. Pupils are advised not to upload personal photos of themselves or others on any social network space without permission.
5. Pupils are advised on security and encouraged to set „strong' passwords, deny access to unknown individuals and instructed how to block unwanted communications.
6. Pupils are encouraged to use privacy settings and invite known friends only and deny access to others if such sites were to be used.

Video Conferencing/ Skype

1. Videoconferencing/skype will only be used in a teacher directed and supervised environment.
2. Staff need to ensure the connection is closed after use.
3. It will only be installed on teacher's main classroom computers.

Managing Mobile and Emerging Technologies (Netbooks, Tablets, Cameras, Mobile Phones)

1. Emerging technologies will be examined for educational benefit and a risk assessment will be discussed by the online safety team before use in school is allowed.
2. All equipment in school is to support the education and wellbeing of our children.
3. Focussed tasks will be provided to the children when allowed on any of these emerging technologies and boundaries set by the teacher.

Mobile Phone / Devices Usage in School

1. Mobile phones and other devices will not be used for personal use during formal school time.
2. Pupils are not allowed to have mobile phones in school.
3. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of the leadership team.
4. Mobile phones are forbidden on trips.
5. Staff Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times in a bag.
6. No images or videos should be taken on any mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
7. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
8. Staff have the right to confiscate and search pupil's devices if a safeguarding incident has been brought to their attention. Any evidence will be taken and stored appropriately.
9. The sending of abusive or inappropriate messages is forbidden.
10. If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office.
11. If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
12. Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Google Education Apps Staff Users

1. At present only staff members of the school use google education apps for communication and sharing purposes.
2. Staff use google email, calendars, documents and sites.
3. No personal data relating to staff or pupils is placed on the application.
4. Only initials or first names of the children are used

5. There are no advertisements used with Google Apps for Education. Gmail offers web clips at the top of the inbox which show you news headlines, blog posts, RSS and Atom feeds. You can choose to Hide all advertisements from the control panel. Additional information on google security and filtering can be found at:
   http://www.google.com/support/a/bin/answer.py?answer=60762
   http://www.google.com/support/a/bin/answer.py?answer=60730

Protecting Personal Data (See Data Protection Policy for Further Details)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

All staff in school must ensure:

1. They take care and safe of all personal data, minimising the risk of its loss or misuse.
2. They send personal data securely off the school site. (See School Business Manager)
3. Use password protected computers and ensure equipment is logged-off at the end of the session where personal information could be accessed or viewed.
4. Transfer or store data using encrypted and secure password devices.
5. Any data transferred is used on a virus protected system which is regularly updated.
6. All data is deleted from the device once transfer is complete.
7. Digital Cameras are cleared before allowing off site and photographs are transferred to the school protected systems.
8. Equipment that is taken off site must be checked that no personal information can be accessed.
9. All devices taken off site, e.g. laptops, tablets, removable media or phones, need to be secure in a locked, safe environment and, for example, not left in cars or insecure locations. All devices should have a passcode on them

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Reporting on progress

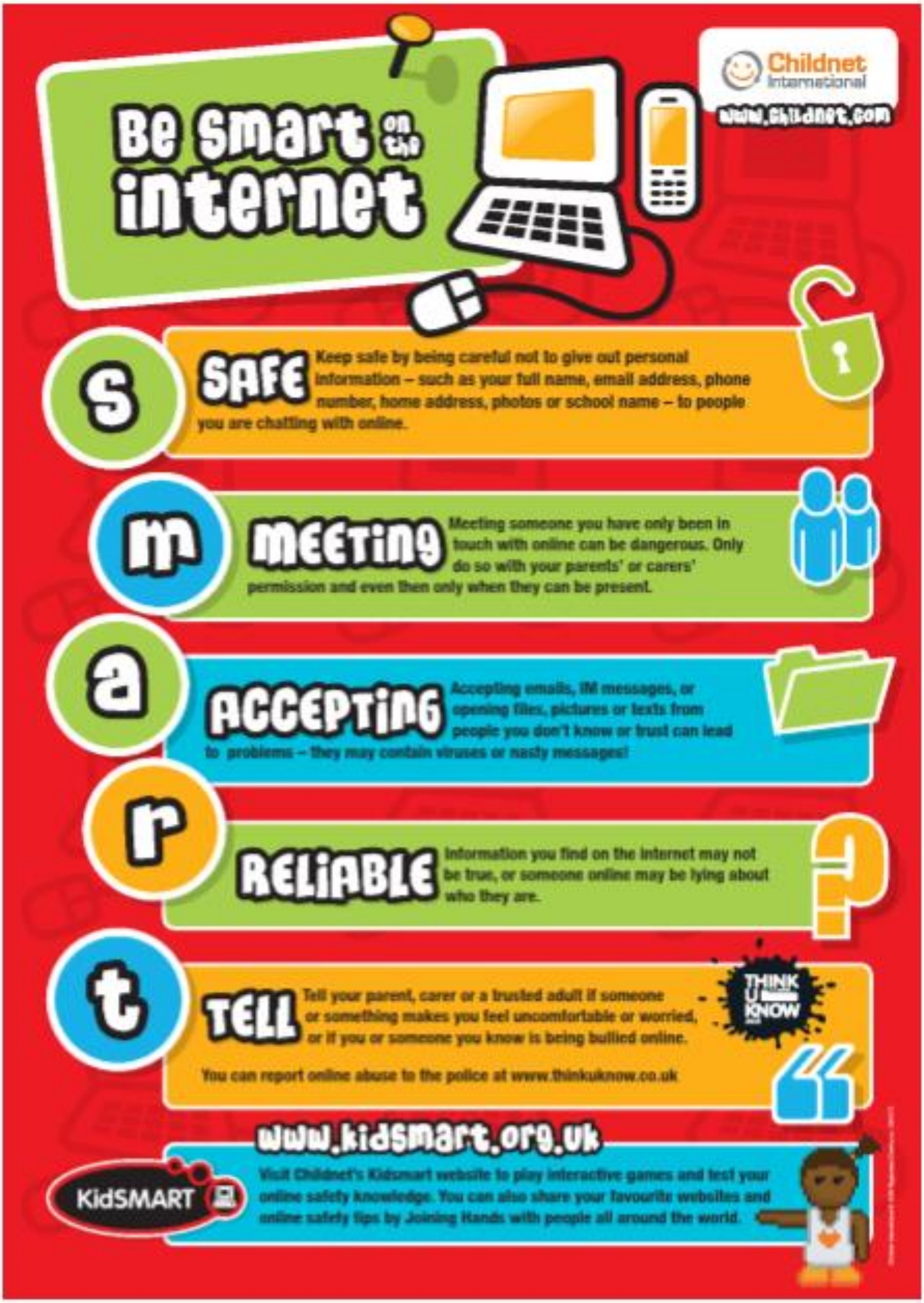
The policy has been distributed, read and agreed by staff.

Online Safety Team	Mo Andrews (Executive Headteacher) Rhea Kurcewicz (Head of School) Deborah Maskrey (Strategic Lead for Safeguarding Karen Stanley (Business Manager) Rob Spencer (Network Manager)
Online Safety Governor	Lucy Davies

This scheme will be reviewed annually and the main findings will be reported to the full governing body.

List of Appendices

SMART Rules for Wall Display – Appendix A



S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

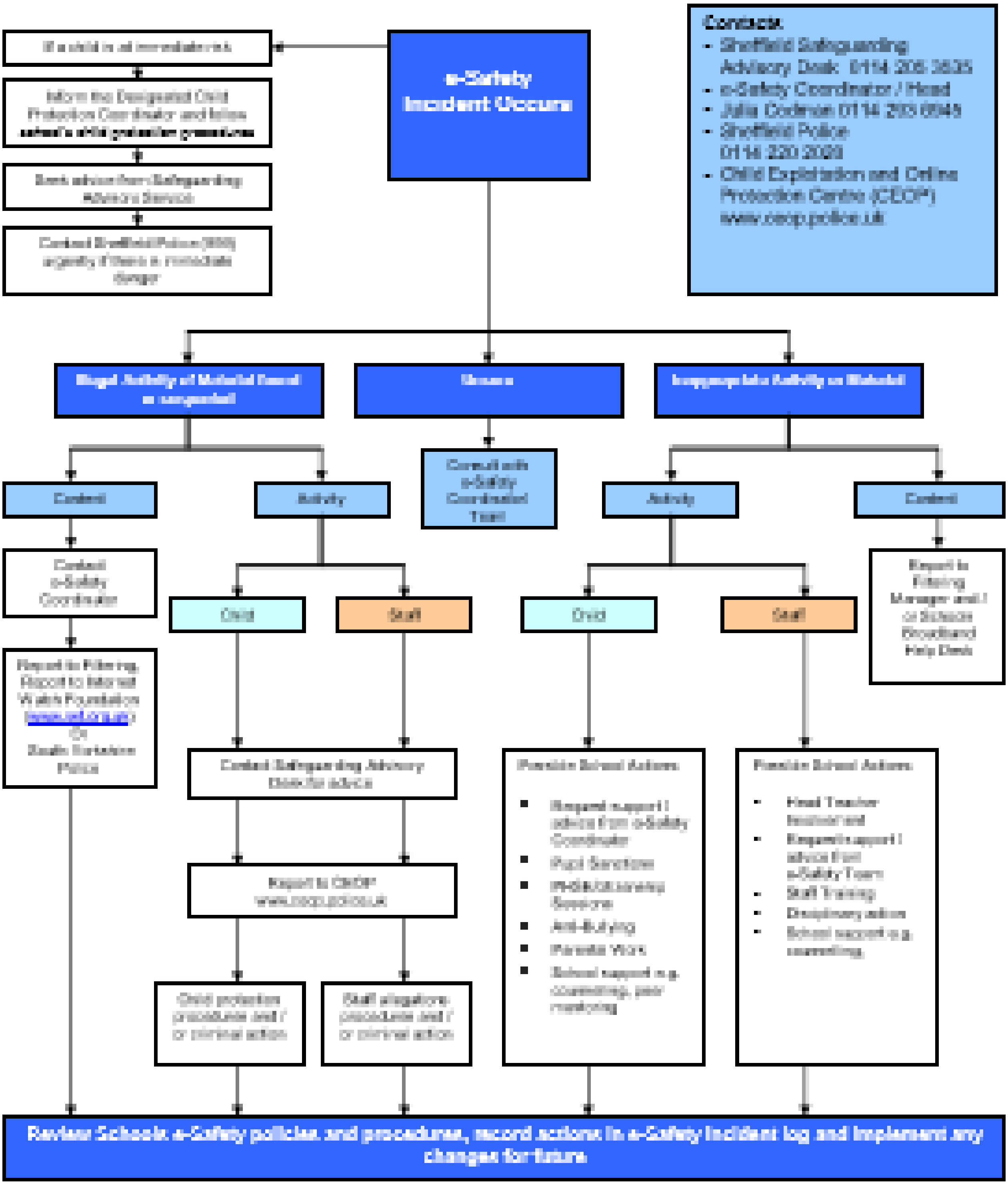
T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Response to an Incident of Concern – Appendix B


If a child is at immediate risk
Inform the Designated Child Protection Coordinator and follow school's child protection procedures
Seek advice from Safeguarding Advisory Service
Contact Sheffield Police (999) urgently if there is immediate danger
e-Safety Incident Occurs
Contacts:
- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Coordinator / Head
- Julia [illegible] 0114 293 [illegible]
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk
Illegal Activity of Material found or suspected
Unsure
Inappropriate Activity or Material
Content
Activity
Consult with e-Safety Coordinator/ Team
Activity
Content
Contact e-Safety Coordinator
Child
Staff
Child
Staff
Report to Filtering Manager and / or Schools Broadband Help Desk
Report to Filtering, Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police
Contact Safeguarding Advisory Desk for advice
Report to CEOP www.ceop.police.uk
Child protection procedures and / or criminal action
Staff allegations procedures and / or criminal action
Possible School Actions:
Request support / advice from e-Safety Coordinator
Pupil Sanctions
PHSE/Citizenship Sessions
Anti-Bullying
Parental Work
School support e.g. counselling, peer mentoring
Possible School Actions:
Head Teacher involvement
Request support / advice from e-Safety Team
Staff Training
Disciplinary action
School support e.g. counselling
Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future

Contact Details

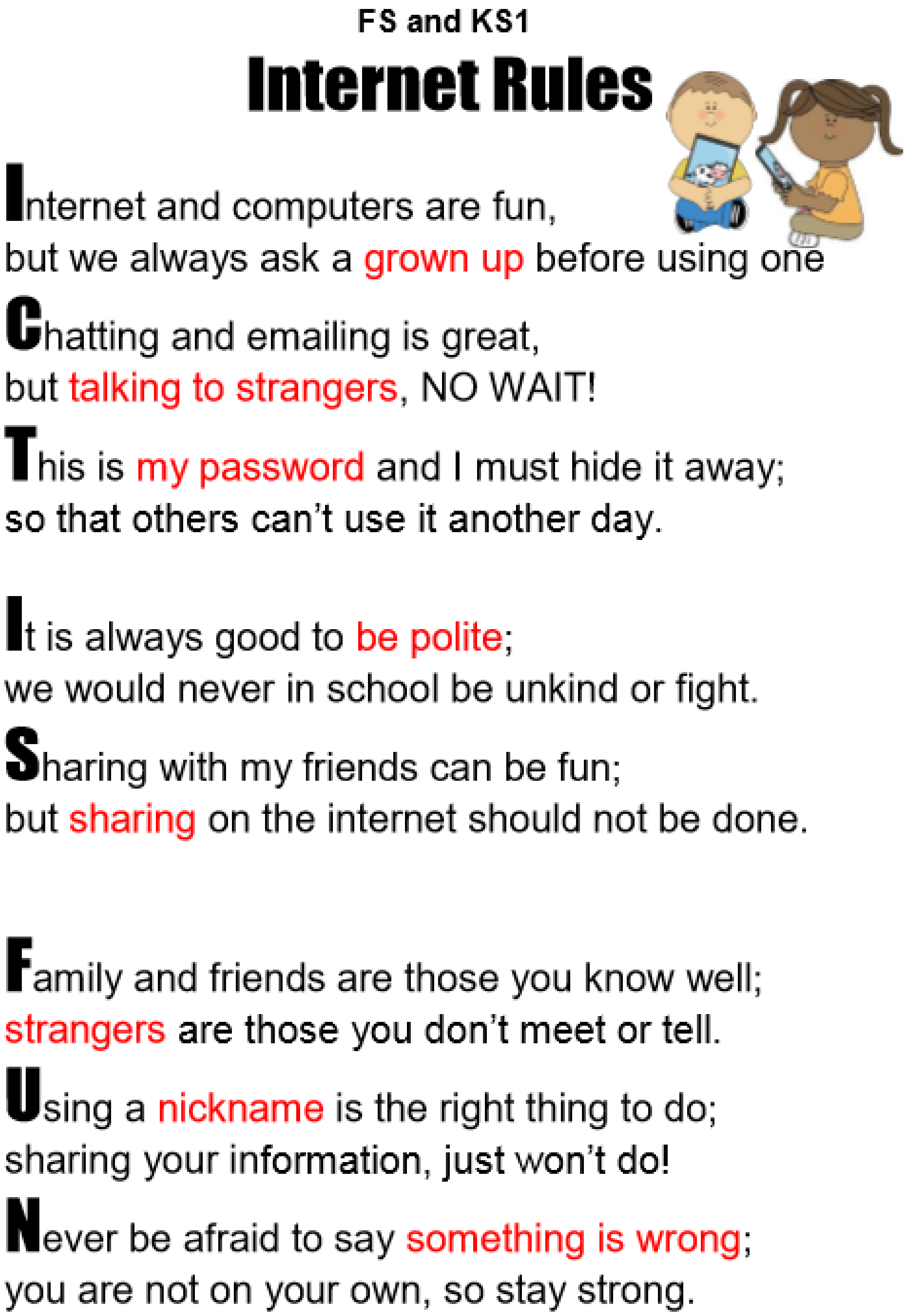
Schools Designated Child Protection Officer: Alan [illegible]/ Peter [illegible]
School e-Safety Coordinator Susan [illegible]/ John Fernandes

Pupil Sanctions.

Reinforce the Acceptable Use Agreements and log incidents.

Give appropriate sanction:
1. Warnings
2. No Internet Activity
3. Inform Head Teacher
4. Inform Parents

Wall Display of Pupil Online safety Rules– Appendix C



FS and KS1

Internet Rules

Internet and computers are fun,
but we always ask a grown up before using one

Chatting and emailing is great,
but talking to strangers, NO WAIT!

This is my password and I must hide it away;
so that others can’t use it another day.

It is always good to be polite;
we would never in school be unkind or fight.

Sharing with my friends can be fun;
but sharing on the internet should not be done.

Family and friends are those you know well;
strangers are those you don’t meet or tell.

Using a nickname is the right thing to do;
sharing your information, just won’t do!

Never be afraid to say something is wrong;
you are not on your own, so stay strong.

KS2 Internet Rules

Think Before You Click!

- We ask permission before using the Internet
- We stay focussed on the tasks set by the teacher
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any sites we are not sure about.
- We only e-mail people an adult has approved.
- We do not open e-mails sent by anyone we don’t know.
- We type messages that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not set up our own profiles without permission
- We do not enter chat rooms or use instant messaging without adult supervision
- We don’t upload images of ourselves or others without permission
- We use an alias name and an avatar when online
- We only use our first name when blogging
- We never complete any forms online
- We acknowledge where we get our images from
- We know not to copy material from the internet as this is plagiarism

Whole School Online safety Rules – Appendix D

Whole School Online safety Rules

These online safety Rules help to protect pupils and the school community by describing acceptable and unacceptable internet use as a visitor, student, guest or staff in our school.

- The school owns the computer network and sets rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal any personal information
- The school IT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- Personal Social Media accounts are not accessed on the school's systems or to be used against the school outside
- Personal devices like mobile phones or tablets are not to be used in classrooms to take images or videos of the children without permission from the class teacher or senior management.

Visitors: …………………………………………..

Date:…………………..

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Pupil Acceptable Use Agreement – Appendix E

Acceptable Use Agreement

I understand that I must use the school's ICT resources in a responsible manner, to make sure that I keep myself and others safe whilst working online.

Personal Safety

- I will keep my passwords safe and will not use other people's passwords
- I will be aware of "stranger danger", when working online.
- I will not share personal information about myself or others when on-line.
- I will not upload any images of myself or of others without permission
- I will not arrange to meet up with people that I have communicated with online.
- I will immediately report any inappropriate material, messages I receive or anything that makes me feel uncomfortable when I see it online.
- I will report any bad behaviour by telling a responsible adult and will learn about using the CEOP Report button.
- I know that the school can look at my use of ICT and what I use online

ICT Property and Equipment

- I will respect all computer equipment and will report any damage or faults.
- I will respect others' work and will not access, copy, move or remove files.
- I will not use mobile phones/USB devices in school without permission.
- I will not use any programs or software without permission.
- I will not use or open email, unless I know and trust the person or organisation.
- I will not install programs or alter any computer settings.
- I will only use approved and moderated chatrooms or social networking sites with permission from a responsible adult

The Internet

- I understand that I need permission to be on the Internet.
- I will not fill in any online forms without adult permission
- I will not use any sites I've not had permission to use, this includes social media sites that I'm not old enough to use

- I will learn about copyright laws and make sure I acknowledge resources
- I will not upload or download images, music or videos without permission
- I will check that the information that I access on the internet is accurate, as I understand that the internet may not be truthful and may mislead me.

Mobile Phones

- I know that mobile phones are not allowed to be in school during the school day.
- I know not to use text, voice messages, take images or use any internet connection to bully, upset or shock anyone in and out of school.
- I know that no images or videos should be taken on any mobile phones or personally-owned mobile devices without the consent of the person or people it involves.
- I know that the school is not responsible for any loss or damage to my mobile phone or any device I bring onto the school site.
- I understand that the school have a right to confiscate, search and keep any evidence on any mobile devices I bring into school.
- I know that I should protect my phone number by only giving them to trusted friends and family.

Cyber Bullying

- I will be polite when I communicate with others
- I know not to do online what I wouldn’t do offline like in the playground
- I will not use inappropriate language or make unkind comments
- I appreciate others may have different opinions
- I will not upload or spread images of anyone

Outside of the School Community

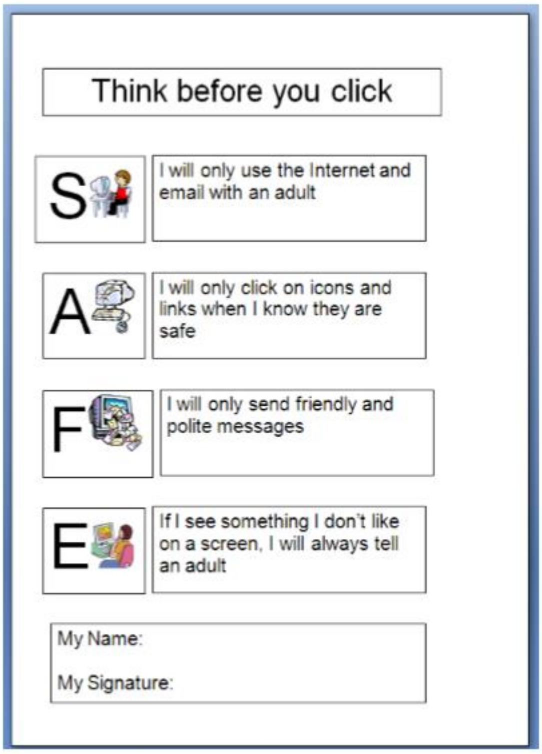
- I understand that this agreement is for in and outside the school
- I know there will be consequences if I am involved in incidents of inappropriate behaviour covered in this agreement

Pupil Acceptable Use Policy Agreement – Years 1-4

Acceptable Use Agreement

This is how we stay safe when we use computers:

- I will ask a teacher / an adult if I want to use the computer.
- I will only use activities that the teacher /an adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from the teacher / an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell the teacher / an adult if I see something that upsets me on the screen.
- I will not bring my mobile phone to school.
- I know not to talk to strangers online.
- I will keep my personal information and passwords safe.
- I will always be nice if I do post or put up messages online.
- I know that if I break the rules I might not be allowed to use the computer.



Think before you click

S	I will only use the Internet and email with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Parent/Carer Acceptable Use Agreement – Appendix F

Parent/Carer Online Safety and Acceptable Use Policies Information

As part of the programme of activities in school, all pupils have the opportunity to access a wide range of communication technology resources. These resources are an essential part of promoting children's learning and development; however, we also recognise the potential risks associated with these technologies. We therefore have an Online Safety and Acceptable Use Policies in place in school.

In recent years, social networking sites such as Facebook and Twitter have grown in popularity and many people use them to communicate with family and friends. The vast majority of people who use social networking show respect in their communication with others and is something we must encourage to show our children that we are positive, digital role models. However, there are times when people disregard the rules and will use social networking sites to cyberbully and harass others.

As a school, we encourage our parents to support us with the education and wellbeing of their children and if at any time, parents feel they have issues regarding their child's education, they should make an appointment with the Head teacher. As a community, we should all frown upon the use of social networking sites by parents to criticise and make unsubstantiated comments about the school or any members of staff.

We do not want to go down the line of sending out legal letters from solicitors to parents about untrue and damaging comments made on social networking sites. Current laws such as the 1988 Malicious Communication Act, 1997 Protection from Harassment Act and 2003 Communication Act can be used to protect people from malicious and threatening posts on the internet.

If an incident is reported to school staff, it should be investigated and, if school deem it appropriate, should be acted upon. In extreme cases, the head teacher would consider whether it appropriate to notify the police to take further action.

Therefore, as a Parent/Carer, you are asked to:

1. **Read the Parent/Carers Acceptable Use Agreement Form Read and talk to your child about their Pupil Acceptable Use Agreement**
2. **Parent/Carer and child to sign the agreement on the enclosed form.**
3. **Return to School as soon as possible.**

There will be an opportunity to attend another parent's Online safety Session at the beginning of the new academic year to inform you of the Online safety issues and risks children face, how we teach Online safety in school and to support any questions you may have.

If you disagree with any of the rules within the agreements or feel there is an area of Internet Safety you feel is not being developed please contact the Headteacher.

Please remember, all children in school are taught how to keep safe and be responsible when they are online, whether they are at school or at home. As children are able to access the internet outside school, whether this is at home, a friend's house or on a mobile device, we need to work in partnership with you the parent/carer to keep our children safe.

Parent / Carer and Pupil Acceptable Use Agreement Form (to be returned)

Parent / Carer Acceptable Use Agreement:

- I have read and discussed the agreement with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.
- 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 agree that the school is not liable for any damages arising from use of the Internet facilities.
- I understand that my son's/daughter's activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the Internet Safety Rules or Pupil Acceptable Use Agreement.
- I understand not to upload any photos of Pye Bank pupils at any school event (for example, assemblies/sports days/plays or school trips) onto a social media site.
- I understand that everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate or malicious comments about the school or any members of the school community.

Parent/carer signature:	Date:

Staff Acceptable Use Policy Agreement – Appendix G

Staff Acceptable Use Policy Agreement

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

1. Systems - I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
2. Misuse - I will ensure that school owned information systems use will always be compatible with my professional role. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. Private Use - I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
4. Logging in/out - To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
5. Passwords - I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word) and update regularly. If I have been given a generic password for first use I will change this immediately.
6. Software - I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission.
7. Copyright - I will respect copyright and intellectual property rights.
8. Data Protection - I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
9. Personal Information - I will not keep professional documents which contain school related sensitive or personal information (including images, files, videos etc.) on any

personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platforms to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

10. Reporting - I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator and/or the online safety Coordinators as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the online safety Team. I know the CEOP Report Button.
11. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the Head Teacher and ICT Technicians.
12. Communication - I will ensure that any electronic communications with pupils and parents are compatible with my professional role.
13. My Professional Role - My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
14. Publishing of Material - I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
15. I will only use my school email account for school business. Any documents which refer to confidential information will be sent securely/password protected.
16. I will not use my personal email for school business.
17. I will not use the school mobile phone for personal use.
18. During school working hours my phone will be stored safely and will be turned off or on silent to prevent disruption to learning. When using my mobile phone for calls during official breaks I will not do so in shared areas, such as the staff room.
19. I will ensure that devices belonging to school (laptops, mobile phones or Ipads) are kept safe at all times. I will not leave them unattended in vehicles.

Teaching Online safety

1. I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

Social Networking Sites

1. The school advises that social networking and media sites are used responsibly. If I do decide to use them, I will ensure that my personal use of these sites is compatible with my professional role and that privacy settings have been set. I am aware that sites are never fully private and that great care is needed when adding content.

2. I will never undermine the school, its staff, parents or children. I know not to become “friends” with parents or pupils on social networks. I will always use my professional code of conduct if a parent relationship pre- existed and will never bring the school in disrepute. I have read and understood the school’s Social Media Policy.
3. I will report any misuse of social networking linked to school staff or stakeholders.

Reporting

1. I will report any incidents of concern regarding children’s or staff safety to the school online safety Coordinator, Child Protection Teacher or Head Teacher.
2. I will report any breaches of the acceptable use policy that I am aware of.

Monitoring - I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

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

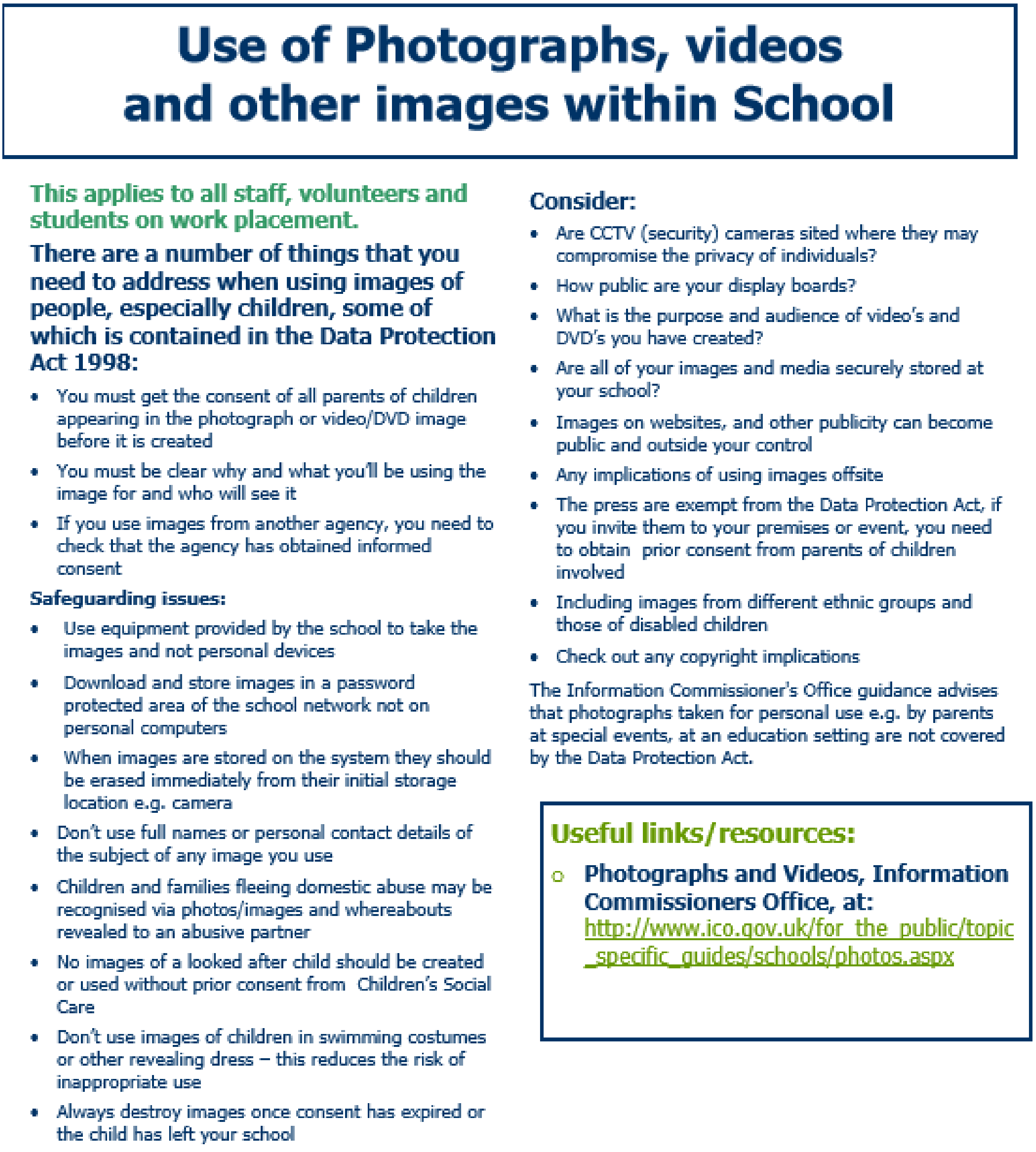
Signed: ……………………………………………..(Printed) …………………………………

Date: …………………… Position within School: ……………………………………………………………….

Online Incident Log Sheet – Appendix H

Online Incident Log Sheet	
Pupil Name	
Class	
Staff name	
Computer in use	
Date of Incident	
Description of incident	
Action taken	
Member of staff reporting/dealing with incident	
Signed	
Date	

Taking Photographs at School Events – Appendix I



Use of Photographs, videos and other images within School

This applies to all staff, volunteers and students on work placement.

There are a number of things that you need to address when using images of people, especially children, some of which is contained in the Data Protection Act 1998:

- You must get the consent of all parents of children appearing in the photograph or video/DVD image before it is created
- You must be clear why and what you'll be using the image for and who will see it
- If you use images from another agency, you need to check that the agency has obtained informed consent

Safeguarding issues:

- Use equipment provided by the school to take the images and not personal devices
- Download and store images in a password protected area of the school network not on personal computers
- When images are stored on the system they should be erased immediately from their initial storage location e.g. camera
- Don't use full names or personal contact details of the subject of any image you use
- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner
- No images of a looked after child should be created or used without prior consent from Children's Social Care
- Don't use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use
- Always destroy images once consent has expired or the child has left your school

Consider:

- Are CCTV (security) cameras sited where they may compromise the privacy of individuals?
- How public are your display boards?
- What is the purpose and audience of video's and DVD's you have created?
- Are all of your images and media securely stored at your school?
- Images on websites, and other publicity can become public and outside your control
- Any implications of using images offsite
- The press are exempt from the Data Protection Act, if you invite them to your premises or event, you need to obtain prior consent from parents of children involved
- Including images from different ethnic groups and those of disabled children
- Check out any copyright implications

The Information Commissioner's Office guidance advises that photographs taken for personal use e.g. by parents at special events, at an education setting are not covered by the Data Protection Act.

Useful links/resources:

○ **Photographs and Videos, Information Commissioners Office, at:** http://www.ico.gov.uk/for_the_public/topic_specific_guides/schools/photos.aspx

Organisations, Documents and Resources – Appendix J

RESOURCES

ThinkUKnow - http://www.thinkuknow.co.uk/
Childnet International - http://www.childnet-int.org/
Kidsmart: http://www.kidsmart.org.uk/default.aspx
Know It All http://www.childnet-int.org/kia/
Cybersmart http://www.cybersmartcurriculum.org/home/
Chatdanger - http://www.chatdanger.com/
Digizen – cyber-bullying films:
http://www.digizen.org/cyberbullying/film.aspx
NCH - http://www.stoptextbully.com/

ADVICE FOR PROTECTING CHILDREN Child Exploitation and Online Protection Centre (CEOP) - http://www.ceop.gov.uk/
The Byron Review ("Safer Children in a Digital World")
http://www.dcsf.gov.uk/byronreview/

CYBER BULLYING
http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/
Cyberbullying.org - http://www.cyberbullying.org/

SOCIAL NETWORKING Digizen – "Social Networking Services" -
http://www.digizen.org.uk/socialnetworking/
DATA PROTECTION Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx