****

Priestthorpe Primary School

E-safeguarding Policy

September 2016- draft

To create a secure and safe environment which develops technology skills and provides pupils with awareness of potential E-Safeguarding scenarios that may arise.

**Policy statement**

New technologies have become integral to the lives of children and young people in today’s society, both outside and within school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve Literacy and communication skills, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

However, the use of these new technologies can put young people at risk both inside and outside of school. Some of these dangers may include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to/loss of/sharing of personal information

• Inappropriate communication/contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video/Internet games

• Potential for excessive use which may impact upon the social and emotional development and learning of the young person

• Plagiarism and copyright infringement

• Illegal downloading of music or video files

• An inability to evaluate the quality, accuracy and relevance of information on the Internet

• The sharing/distribution of personal images without an individual’s consent or knowledge

• The risk of being subject to grooming by those with whom they make contact on the Internet

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils’ awareness to the risks which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.

**Development / Monitoring / Review of this Policy**

4

This e-safety policy has been developed by an E-safety group made up of:

*• Headteacher*

*• E-Safety Coordinator*

*• Staff – including Teachers, Support Staff, Technical staff*

*• Governors*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This e-safety policy was approved by the *Board of Directors /* *Governing Body / Governors Sub Committee on:* | *Insert date* |
| The implementation of this e-safety policy will be monitored by the: | *Insert name of group / individual (suggested groups – E-Safety Coordinator / Officer / Committee, Senior Leadership Team, other relevant group)* |
| Monitoring will take place at regular intervals: | *Insert time period (suggested to be at least once a year* |
| The *Board* *of Directors* / *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | *Insert time period (suggested to be at least once a year* |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *Insert date* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Insert names / titles of relevant persons / agencies eg: LA ICT Manager, LA Safeguarding Officer, Police*  |

The school will monitor the impact of the policy using:

*• Logs of reported incidents*

*• Monitoring logs of internet activity (including sites visited)*

*• Internal monitoring data for network activity*

*• Surveys / questionnaires of*

*• pupils*

*•* parents / carers

*• staff*

**Scope of the Policy**

This policy applies to all members of the *school* community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

**Roles and Responsibilities**

7

The following section outlines the e-safeguarding roles and responsibilities of individuals and groups within the *school*:

**Governors:**

Governorsare responsible for the approval of the E-safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governorsreceiving regular information about e-safeguarding incidents and monitoring reports. A member of the Governing Body has taken on the role of E-safeguarding Governor.

The role of the E-Safeguarding *Governor* will include:

*• regular meetings with the E-Safeguarding Co-ordinator*

*• regular monitoring of e-safeguardingincident 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 e-safeguarding) of members of the school community**, though the day to day responsibility for e-safeguarding will be delegated to the *E-safeguarding Co-ordinator*.

• **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 e-safeguarding allegation being made against a member of staff.** (see flow chart on dealing with e-safeguarding incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority HR / other relevant body* disciplinary procedures).

*• The Headteacher and Senior Leaders are responsible for ensuring that the E-safeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safeguarding 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 e-safeguarding 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 E-safeguarding Co-ordinator.*

**E-safeguarding Coordinator / Officer:**

• leads the e-safeguarding committee

• takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policies / documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safeguarding incident taking place.

• provides training and advice for staff

• liaises with the Local Authority / relevant body

• liaises with school technical staff

• receives reports of e-safeguarding incidents and creates a log of incidents to inform future e-safeguarding developments, (Examples of suitable log sheets may be found later in this document). SWGfL BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents ([http://www.swgfl.org.uk/Staying-Safe/E-safeguarding-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper](http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper))

• meets regularly with E-safeguarding *Governor*  to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting / committee of *Governors*

• reports regularly to Senior Leadership Team

**Network Manager / Technical staff:**

The *Network Manager / Technical Staff / Co-ordinator for ICT / 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 e-safeguarding technical requirements and any *Local Authority / other relevant body* E-safeguarding Policy / 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 e-safeguarding technical information in order to effectively carry out their e-safeguarding role and to inform and update others as relevant

• that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the  *Headteacher / Senior Leader; E-safeguarding Coordinator* for investigation / action / sanction

*• that monitoring software / systems are implemented and updated as agreed in school policies*

**Teaching and Support Staff**

are responsible for ensuring that:

**• they have an up to date awareness of e-safeguarding matters and of the current *school* e-safeguarding 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 ; E-safeguarding Coordinator* for investigation / action / sanction**

**• all digital communications with pupils / parents / carers should be on a professional level** *and only carried out using official school systems*

• e-safeguarding issues are embedded in all aspects of the curriculum and other activities

• pupils understand and follow the e-safeguarding and acceptable use policies

• 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 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*

**Child Protection / Safeguarding Designated Person / Officer**

should be trained in e-safeguarding issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

**Pupils:**

**• are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**

• 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 cyber-bullying.

• should understand the importance of adopting good e-safeguarding practice when using digital technologies out of school and realise that the *school’s*  E-safeguarding Policy covers their actions out of school, if related to their membership of the school

**Parents / 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, newsletters, letters, website / VLE and information about national / local e-safeguarding campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-safeguarding practice and to follow guidelines on the appropriate use of:

**•** digital and video images taken at school events

• access to parents’ sections of the website / VLE and on-line pupil records

• their children’s personal devices in the school (where this is allowed)

**Community Users**

Community Users who access school systems / website / VLE as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

**E-safeguarding Group**

The E-safeguarding Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding e-safeguarding and the monitoring the e-safeguarding policy including the impact of initiatives. Depending on the size or structure of the *school* this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body.*

Members of the *E-safeguarding Group* will assist the *E-safeguarding Coordinator* with:

• the production / review / monitoring of the school e-safeguarding policy / documents.

*• the production / review / monitoring of the school filtering policy and requests for filtering changes.*

*•* mapping andreviewing the e-safeguarding curricular provision – ensuring relevance, breadth and progression

*•* monitoring network / internet / incident logs

*•* consulting stakeholders – including parents / carers and the pupils about the e-safeguarding provision

*•* monitoring improvement actions identified through use of the 360 degree safe self- review tool

Policy Statements

Education – pupils

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

**E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

**• A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**

**• Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**

**• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**

**• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**

*• Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*

*• Staff should act as good role models in their use of digital technologies the internet and mobile devices*

*• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*

*• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

Education – parents / carers

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

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

*• Curriculum activities*

*• Letters, newsletters, web site, VLE*

*• Parents / Carers evenings / sessions*

*• High profile events / campaigns eg Safer Internet Day*

*• Reference to the relevant web sites / publications*

Education – The Wider Community

*The school will provide opportunities for local community groups / members of the community to gain from the school’s e-safety knowledge and experience. This may be offered through the following:*

* *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
* *E-Safety messages targeted towards grandparents and other relatives as well as parents.*
* *The school website will provide e-safety information for the wider community*
* *Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision*

Education & Training – Staff / Volunteers

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

• **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-safety as a training need within the performance management process.*

**• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**

*• The E-Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*

*• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*

*• The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

**Governors / Directors should take part in e-safety training / awareness sessions**, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).

• Participation in school training / information sessions for staff or parents

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

**• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**

•In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.

• *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*

• *Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*

• *Pupils must not take, use, share, publish or distribute images of others without their permission*

• *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*

• *Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.*

• *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website*

• *Pupil’s work can only be published with the permission of the pupil and parents or carers.*

Pupil Acceptable Use Policy Agreement Template

for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adultif I want to use the computers

I will only use activities that a teacher or suitable adulthas told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adultif I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adultif I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

*Signed (child):……………………………………………*

Signed (parent): …………………………………………..

Pupil Acceptable Use Agreement Template

for older pupils

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy 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 users at risk.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

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

**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, financial details etc )

• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

**I understand that everyone has equal rights to use technology as a resource and:**

• I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

• 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 use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

25

**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 and to ensure the smooth running of the *school*:**

• I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

• 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 open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 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 only use social media sites with permission and at the times that are allowed

**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 the *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, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

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

Pupil Acceptable Use Agreement Form

This form relates to the *pupil* Acceptable Use Agreement, to which it is attached.

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

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

• I use the *school* systems and devices (both in and out of school)

• I use my own devices in the *school*  (when allowed) eg mobile phones, gaming devices USB devices, cameras etc

• I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Class

Signed

Date

Parent / Carer Countersignature

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today’s society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

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 / academy ICT 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 ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

• I understand that the *school* will monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school

• I understand that the school ICT 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)

• 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.

28

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

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

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only use chat and social networking sites in school in accordance with the school’s policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)

• I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)

• I will not engage in any on-line activity that may compromise my professional responsibilities.

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

• When I use my mobile devices (PDAs / 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 use personal email addresses on the school ICT systems.

• 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. (schools should amend this section in the light of their policies on installing programmes / altering settings)

• 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 / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

• I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school 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 ICT equipment in school, but also applies to my use of school ICT 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 (schools should amend this section to provide relevant sanctions as per their behaviour policies) 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 ICT 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

Use of Digital / Video Images

24

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above *pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed

Date