Western Road CP School

Computing, E-safety and Cyberbullying Policy 2015/16

Adopted February 2016

Introduction:

Western Road CP School is committed to developing the safe use of computing technologies throughout the school organisation and developing skills of staff, students and the wider community.

The use of computing technologies within Western Road CP School is currently developing and the curriculum now reflects and supports this development. Our curriculum will support and assist students in their day-to-day learning and help them make varied and safe uses of technology.

Objectives:

It is our aim to provide all children with:

- the knowledge, understanding and skill so that they can fulfil the requirements of the Foundation stage and National Curriculum;
- equal access to computing facilities;
- opportunities to analyse problems in computational terms and have repeated practical experience of writing computer programs in order to solve such problems;
- the ability to evaluate and apply IT, including new or unfamiliar technologies, analytically to solve problems;
- the skills and knowledge to be responsible, competent, confident, creative and safe users of technology.

Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of World Wide Web content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use. Websites to be used during a lesson or recommended for Home Learning should be checked prior to use for inappropriate content, e.g. advertisements, although it is acknowledged that these can change between this check and the site being used by pupils.

- The school provides access to YouTube as a learning resource. Children are not allowed to access this website. When teachers use this resource they should follow these guides – watch the complete clip/programme prior to showing it to the class. This is to ensure the material has not been tampered with and remains suitable for viewing. Teachers should also ensure they have “autoplay” (found on the far right of the viewing screen) turned off and “Restricted Mode” is “ON”. These measures will reduce but not completely stop the possibility of inappropriate material to be viewed through the YouTube service.

- The school audits computing use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

The Curriculum:

The curriculum should inspire and challenge all learners and prepare them for the future. The school’s aim is to develop a coherent curriculum that builds on young people’s experiences in the primary phase and that helps all young people to become successful learners, confident individuals and responsible citizens. Staff will be supported in developing these lessons and achieving the objectives of the National Curriculum by having the opportunity to access the ‘Switched On Computing’ scheme of work published by Rising Stars. The aim of the scheme is to develop pupils understanding of the concepts, practices and perspectives that underpin programming and other aspects of computer science, while providing ample opportunity for creative, collaborative project work in which pupils can acquire the skills they need.

The scheme offers cross curricular links and differentiation opportunities however teachers do have the freedom to adapt and amend these to make them match their individual classes needs and may therefore use the scheme as a means to identify that they have covered the curriculum.

All children in the school will find the E-Safety is embedded through the teaching and use of computing and online systems, with staff reinforcing E-Safety messages across the curriculum. In addition to this there is planned E-Safety curriculum that is broad, relevant and provides progression, with opportunities for creative activities this will be provided in the following ways:

- A planned E-Safety curriculum should form part of Computing/PSHE and be regularly visited where opportunities allow.
- Key safety messages should be reinforced as part of a planned programme of assemblies and targeted activities.
- Pupils should be taught in all lessons to be critically aware of the materials /content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information and to respect copyright when using material accessed on the world-wide web.

- Students 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 the school.
- Staff should act as good role models in their use of digital technologies, the world-wide web and mobile devices
- In lessons where the 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 – see Appendix 3.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites visited.
- It is accepted that from time-to-time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked appropriate requests should be made to the Headteacher and Computing Co-ordinator to authorize the temporary unblocking of certain sites. This request must document why only this site, not an already authorized site, can provide the learning we are hoping to achieve.

With computing becoming an ever greater part of adult and secondary life it is important that we equip all children with the skills necessary to operate in these worlds. Key Stage 2 will now be working to improve students keyboard skills dedicating 10 – 15 minutes a week to the touch type program offered by BBC Bitesize Dance Mat Typing www.bbc.co.uk/guides/z3c6tfr. Once children become familiar with the process of typing it may at a later stage be necessary for us to invest in a scheme that requires us to pay to support learners development of keyboard skills – consideration should be made of "English Type" www.englishtype.com/schools.php and other similar programs.

All children are given equal access to computing. Differentiation is often by support or outcome and children with special needs often use technology to enhance their learning in other areas of the curriculum.

By following this program it will enhance the learning for those with fine motor control giving them skills that they can draw upon to enable engagement with writing.

Organisation and Resources:

Each classroom and the area overlooking the stage (formally the Computer Suite) are equipped with a SMART interactive whiteboard and projector.

Every teacher in the school has access to either their own laptop or laptop within their classroom. Should any teacher or member of staff wish to remove their laptop or any other digital equipment from site they MUST agree this in advance with their line manager and sign out the device with the office administrator. On returning the item the device will be signed back into the school.

We currently have available 30 laptops in Key Stage 1 and Foundation Stage (4 will be set up in the Reception class room on a permanent basis although they will be released if Year 1 or 2 require all 30 for specific learning) Key Stage 2 currently have 30 laptops with an assigned time for discreet computing lessons. The laptops can be booked outside these times by writing on the staff room whiteboard on the day they are required; along with the times and amount of laptops needed. Years 2 – 6 also have access to at least 3 Netbooks in their classrooms. The school has invested in a number of I-Pads and should explore ways to make more effective use of these mobile devices (see Focus Group).

All these computers are connected to the Internet through a network driven by the schools server. All computers are connected to 2 photocopiers via the school network. Print jobs are held in a menu system until requested by staff using a Personal Identification Number – either on their laptops (Konica) or on the printer (Riso).

The school currently has 4 digital cameras – 3 in Foundation and Key Stage 1 and the fourth in Year 5. All cameras have a memory card and charge pack for their batteries (we will explore purchasing more digital cameras for the remaining year groups).

Pupils should be taught to handle all equipment responsibly and safely. With reference to laptops the following guidelines should be observed; Reception laptops should be set-up and shut down by the Class Teacher or Teaching Assistant. It is imperative that laptops be 'shut down' and charged at the end of the day, in every class, to maintain network integrity - never just close the lid. In Year 1, children should learn to remove and transport laptops safely to their tables, Teachers and or Teaching Assistants should ensure all laptops are properly 'shut down' and returned to charge points. In Year 2 and 3, children should learn to remove laptops from the appropriate trolley in a safe manner and while under supervision be taught how to safely return and charge the laptop (by the end of Year 3 pupils should be able to achieve this independently). In Year 4 and above children should be able to also move the Acer trolley, with supervision where necessary, this should only be done with a minimum of 4 children. One child to push, one to pull and guide, one to carry the power cable so that it does not become trapped and one to hold doors open. Teachers may wish to consider computer monitors who will be responsible for the safe and good use of the equipment. If teachers are concerned about their class or individuals ability to achieve any of these tasks they should not allow pupils to carry tasks out independently. The Computing Lead will monitor trolley's and if a class/es are found not to be using the computers responsibly and within these guidelines use will be restricted accordingly – this may involve adults only being allowed to bring and return laptops. Teachers and / or Teaching Assistants in EYFS, Key Stage 1 and 2 should always ensure that laptops are shut down, returned neatly and placed on charge at the end of each session of use. Should updates need to take place this should be allowed to take place before closing and returning the laptop.

The Computing budget is managed by the Computing Lead in consultation with the school Bursar and Head Teacher.

Computing network is maintained by ICT Schools services whom have remote access to the whole school network and have the ability to resolve some technical problems by ‘dialing’ into our computers (using our computer ids) to resolve our technical issues. In doing so small amounts of data maybe removed from our servers for the purpose of diagnostic, this data will be treated as sensitive information and secured by ICT Schools Services and deleted after they have finished using the information. ICT Schools Services are responsible for maintaining our computing infrastructure, firewall, general equipment (hard and software) and virus protection.

Western Road CP School has purchased the ‘Premier’ service with ICT Schools Service; this allows for unlimited on-site technical visits, Office 365 support, Strategic Planning Advice, Curriculum Technical Support, Service Reviews (every 2 terms), Computer Installations, Remote Support, SIMS support, Remote Software Installation, Dedicated Helpdesk, Bespoke Contact Tool and 10 Training Credits.

In order to report a fault teachers and or support staff are requested to make this by logging jobs through the ICT Schools contact tool found on all school laptops or desktops.

ICT Schools will be asked to set the system to create an automatic password renewal for: SIMS, Network access and email at 60 days. This will ensure compliance with Local Authority guidelines found at:
https://czone.eastsussex.gov.uk/schoolmanagement/ict/sims/simsgateway/Documents/Passwords.doc
Password renewal will form part of the User Agreement found in Appendix 2. Staff will be given guidance to the following password recommendations in a separate memorandum;

- Passwords for SIMS, Network Access and email must be changed every 60 days,
- Accounts will be locked after 3 incorrect password entries
- The new password must contain at least 2 different characters from the old password.
- The password must be created from a mixture of upper and lower case letters with at least 2 numbers that is a minimum of 8 characters long,
- An old password will not be allowed to be reused for 12 months

The computing lead and E-Safety body in consultation with the Leadership team and teachers will explore how the “Supply” log-in can be given restricted access to the school network while still allowing supply teachers to carry out their duties.

Printing from I-Pads: it is likely that when using I-Pads teachers may want to print various photos - this is encouraged and welcomed to showcase the learning throughout the school. In order to minimize costs and save resources staff are required, where printing more than one or multiple copies not of A4 size, to first be transfer images to their laptop and then print from their laptop to the desired printer. This process will allow teachers to print more than one image on the page. I-Pads with our current network configuration do not allow for multiple copies to be produced on one page and printing from the I-Pads is therefore causing an increase in paper costs and wastage.

It is expected that from time-to-time teachers will want to access information from school at home. In these circumstances teachers should where possible use the Remote Connection tool to achieve this, thereby maintaining all information within the confines of the school. Where this is not possible then information should be contained on an Encrypted Memory Stick with the encryption activated – merely being in possession of an encrypted memory stick does not encrypt the information.

Staff training:

Professional development will be a priority throughout the 2015/16 school year. After staff complete a Computing survey, a programme of staff development will be created by the computing lead – that may involve external trainers attending staff meetings or inset days – in order to develop all teachers subject knowledge and confidence in the delivering of a curriculum that challenges and supports all of our learners.

Staff will be required to confirm that the training has taken place by signing a 'Computer Skills Training' form located in the Computer Subject Leader folder on the staff drive. Records of staff training will be passed to and kept by the Bursar who will ensure that appropriate annotations of staff personnel files are made.

Taking and use of digital images[1]:

All parents or carers will be given the opportunity to advise the Western Road CP School if they do not wish their child's image to be used on the school website, this will letter will initially be sent out in Reception and be kept on the child's file until they leave Western Road CP School by the Administrator. Any children who join the school during the school year will be given a Digital Image letter as part of their welcome pack to be returned to the school. Failure to return the form will lead to implied consent that the child's image can be used in line with this and the Teaching and Learning policy.

[1] For the purposes of this document 'Digital image' includes any photos or videos captured using any form of digital image capturing technology including but not exclusively camera, video, CCTV

Used images will **never** have a child's full name attached. In most circumstances (always on the website) the label with an image/s will be generic i.e. Larch class…, the Football team… girl/boy…; the only exception to this will be at the Headteacher's discretion, where parents are consulted prior to publication on the website. Children who receive the Headteacher's Award are expected to have their images published in the school newsletter (digital and hard copy) with first names attached to their year group. If any parent or carer does not wish their child's name to be published for this purpose they should contact the Headteacher directly.

Any staff wishing or needing to take images of Western Road CP School children for use in school, on the school website or on the VLE (see below) should do so on **equipment that does not leave the school premises,** unless on an official school excursion. Mobile phones should not be used unless the circumstances are extreme and where it is not practical to use any other device i.e. creation of false holograms when studying light in science. These images should then be deleted once the learning is completed.

From time to time Western Road CP School is host to student teachers who may need to take digital images that form a part of their course or portfolio. As the images are likely to be taken away from Western Road CP School and used for unspecified period of time these guidelines should be followed – is the child's image approved to be used (see Digital Image list held in the school office or with the Computing Co-ordinator), secondly, the students mentor should have a request made of them and note this request and discussion (if the mentor is unsure about if the request can be approved firstly check that the which children's images are prohibited from being used and then seek approval from the Headteacher or Deputy Headteacher. In all circumstances the student should be made aware that the child's name cannot be used in conjunction with any image or video. These same guidelines should be followed for those members of staff wishing to use digital images in their portfolio.

It is common place for parents or carers to want to capture memories in digital form when at school performances, sporting events or celebration of achievements – the school recognises that we do not wish to restrict these individuals unnecessarily and so allow for these images to be taken – the only restriction we place is that these images should **never** be shared on social media, file sharing or video or photo sharing sites in order to maintain all children's rights to privacy. Should the school become aware that this request is being contrived the policy maybe reviewed and amended accordingly to protect all children at Western Road CP School.

Podcast or webcasts will be afforded the same privilege of protection as digital images.

Website and VLE (Virtual Learning Environment):

The Western Road School Website is the front facing domain of the school that members of the public may access and view. In essence it is a tool for marketing the school and quickly informing parents or carers of forth-coming events. The site includes Newsletters, other non-confidential letters disrupted throughout the year in PDF format, Government required policies, the school calendar with upcoming events, summaries of the learning journeys our classes will participate in throughout the year, welcome PowerPoints depicting the way learning will take place throughout the year, links to the class' VLE pages (requiring secure login), details of all staff in the school including the governing body, contact information for the school, an analysis of how we have spent pupil premium monies. The website will also play host to a small number of digital images that promote life at Western Road CP School. The site will be maintained by the Computing Co-ordinator and Office Administrator.

The Western Road CP School VLE is managed through E-Schools. Each member of school staff, pupils, parents, carers and governing body are issued with a username and password. At this time usernames and passwords have only been issued to pupils and staff. The Computing Co-Ordinator and those with Administrator rights have access to all login information and are able to reset any passwords or deny access where abuse of the VLE is determined. Each class teacher has been provided their class usernames and passwords, and distributed these accordingly.

Each class teacher maintains their own page:

Uploading work and pictures or video to showcase learning

Give hints and tips to learning

Setting homework through the VLE – see Learning Policy

Discussion boards will be managed by classteachers, it is recommend that teachers check these daily rather than having to sift through large amounts of discussions after a week of not having contact, little and often (although if you find your class do not use the discussion board as much as others it could be possible to go 2 or 3 days without concern). Children will also be motivated to see teachers involved by responding to work based discussions – this in turn will model good netiquette and online behaviour to your class.

Class page should be updated to reflect the new learning topic within 2 weeks of term commencing. It is recommended that teachers try to spend 10 – 15 minutes every week adding an image (still or moving) to their pages. This will make the page active and live making children want to engage with them rather than pages just being there unused for the term. For us and our learners to get the most from the pages we must show they are living breathing creations that reflect the learning in our classrooms. Again little and often will prove best here as it is quick to upload 2 images or piece of text but takes longer to upload everything done throughout the term. The minimum standard for a class page is: to include a summary of the terms learning, a basic weekly time table, and photos and web links relevant to the current learning.

E-Safety and Cyberbullying[2]:

(This section should be read along with the Child Protection and Anti-Bullying policies).

Western Road CP School believes that everyone in the school community has the right to learn and to teach in a supportive and caring environment without fear of being bullied. We are committed to helping all members of the school community to benefit from computing and online technologies, whilst understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly.

Aims:

This section aims to ensure that:

1. Pupils, staff and parents know about cyberbullying and its consequences;

[2] Cyberbullying will also include the now illegal action of sexting. In the event that sexting is believed or discovered, the procedures for managing and supporting victims described here and in supporting documents should be followed. The action taken against the perpetrator or perpetrators should be in line with Appendix 4 and this section of the policy. Education of sexting should be reviewed by classteachers on a class by class basis, discussed as referred to in the SRE Policy and in terms of E-Safety in the context of illegal actions, cyberbullying, individuals' digital footprints and personal reputation.

2. We have the knowledge, policies and procedures to prevent and, if necessary, to deal with cyber bullying in school or within the school community;

3. We monitor the effectiveness of our procedures.

What is cyberbullying?

- Cyberbullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology such as inferred and Bluetooth.
- It can take many forms, but can go even further than face to face bullying by invading home and personal space and can target one or more people.
- It can take place across age groups and target pupils, staff and others.
- It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.
- It can include messages intended as jokes, but which have a harmful or upsetting effect.

Cyberbullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages;
- Threatening or embarrassing pictures and video clips via mobile phone cameras;
- Silent or abusive phone calls or using the victim’s phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else’s name;
- Menacing or upsetting responses to someone in a chat-room or discussion board;
- Unpleasant messages sent during instant messaging (IM);
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook)

In some cases this type of bullying can be a criminal offence.

Prevention of Cyberbullying:

Understanding and information

- The Computing Co-ordinator, Headteacher, SENCO and Nathan Archer (Governor) will act as an E-Safety Officers, to oversee the practices and procedures outlined in this policy and monitor their effectiveness.
- The E-Safety Officers will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying.
- Staff will be trained to identify signs of cyber bullying and will be helped to keep informed about the technologies that children commonly use.
- A Code of Advice (see Appendix 1) will be developed, periodically reviewed and communicated to help pupils protect themselves from being caught up in cyberbullying and to advise them on reporting any incidents.
- Pupils will be informed about cyberbullying through PSHE, Computing lessons, Assemblies, Anti-Bullying and Computer safety weeks.
- Pupils and staff are expected to comply with the relevant school's Acceptable Computer Use Policy (See Appendix 2).
- Parents will be provided with information and advice on cyberbullying.

Practices and Procedures:

- The responsibilities of the school and of pupils as set out in the Anti-Bullying Policy apply also to this policy.
- Positive use of computing and online technologies will be promoted and the Acceptable Computer Use Policy will be kept under review as technologies develop.
- CPD and INSET will be used to help staff develop their own practices and support pupils in safe and responsible use of technology.
- The school will encourage safe use of online technologies, emphasising, for example, the importance of password security, the need to log out of accounts and netiquette.
- The school will promote the message that asking for help is the right thing to do and all members of the school community will be informed how cyberbullying can be reported.
- Confidential records will be kept of all cyberbullying incidents.

Responding to cyberbullying:

Cyberbullying will generally be dealt with through the schools Anti-bullying policy. A cyberbullying incident might include features different to other forms of bullying, prompting a particular response. Key differences might be:

- Impact: possibly extensive scale and scope
- Location: the anytime and anywhere nature of cyberbullying
- Anonymity: the person being bullied might not know who the perpetrator is
- Motivation: the perpetrator might not realise that their actions are bullying
- Evidence: the subject of the bullying will have evidence of what happened

Support for the person being bullied:

As with any form of bullying, support for the individual will depend on the circumstances.

Examples include:

- Emotional support and reassurance that it was right to report the incident
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff
- Advice on other aspects of the code to prevent re-occurrence
- Advice on how the perpetrator might be blocked from the individual's sites or services
- Actions, where possible and appropriate, to have offending material removed
- Advice to consider changing email addresses and/or mobile phone numbers
- Discuss contacting the police in cases of suspected illegal content see The Protection from Harassment Act 1997, The Malicious Communications Act 1988. Section 127 of the Communications Act 2003; can be used to combat cyberbullying and can result in fines of imprisonment for up to 6 months.

Investigation:

Again, the nature of any investigation will depend on the circumstances. It may include, for example,

- Review of evidence and advice to preserve it, for example by saving or printing

(e.g. phone messages, texts, emails, website pages, blogs and discussion boards)

- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used. Witnesses may have useful information.

- Contact with the Internet Watch Foundation or the police may also be considered. If images could potentially be illegal or raise child protection issues the relevant child protection policy should be read along with this policy.

- Requesting a pupil to reveal a message or other phone content or confiscating a phone. **Staff do not have the authority to search the contents of a phone**.

Working with the perpetrator:

Work with the perpetrator and any sanctions will be determined on an individual basis, in accordance with the Anti-Bullying Policy, with the intention of:

- Helping the person harmed to feel safe again and be assured that the bullying will stop.

- Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour.

- Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour.

- Demonstrating that cyber bullying, as any other form of bullying, is unacceptable and that the school has effective ways of dealing with it.

Evaluating the effectiveness of counter bullying procedures:

- Members of staff will report any incidents of cyberbullying to the Headteacher.

- The Headteacher will review any serious incident within three months of the school dealing with any reported cases and will ensure that an annual review of Cyberbullying and the Anti-Bullying procedures are carried out.

- The review will take into account comments and suggested areas for improvement from staff and students, including input from the School Council.

ROLES AND RESPONSIBILITIES:

The following section outlines the E-Safety roles and responsibilities not already referenced for individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This responsibility lies with the Computing Link Governor who will undertake:

- regular meetings with the Computing Co-ordinator;
- regular monitoring of any E-Safety incidents
- reporting to relevant Governors meeting.

Headteacher and Senior Leadership Team:

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, although the day-to-day responsibility for E-Safety will be delegated to the E-Safety Officers.
- The Headteacher and at least one other member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff see "What we do if" Appendix 3 and "Responding to incidents of misuse" Appendix 4).
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Officers and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure a system of monitoring and support for those in school who carry out the internal E-Safety monitoring role. This will be achieved through regular monitoring meetings with the E-Safety Officers.

E-Safety officer (Computing Co-ordinator):

- takes day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies and documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place;
- undertakes an annual audit of staff training needs for discussion with Governors
- provides training and advice for staff;
- liaises with ICT Schools Services and technical staff;
- Ensures ICT Incidents are logged – in guidance with Child Protection Officer.

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of E-Safety matters and of the current school E-Safety policy and practices;
- they have read, understood and signed the relevant Staff Acceptable Use Policy in Appendix 2

- they report any suspected misuse or problem to the Headteacher and E-Safety Officer for investigation and action;
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems;
- E-Safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the E-Safety 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; and
- 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 Officer:

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

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate online contact with adults / strangers;
- potential or actual incidents of grooming; and
- cyberbullying.

Pupils:

- are responsible for using the school digital technology systems in accordance with the relevant Pupil Acceptable Use Policy in Appendix 2 and:
- 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 cyberbullying; and
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents or Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and / or mobile devices in appropriate way. Parents and carers will be encouraged to support the school in promoting good E-Safety practices and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website/blog
- Their children's personal devices in the school (where this is allowed).

Western Road CP School will take every opportunity to help adults understand these issues through: parents' evenings, newsletters, website, and information about national/local E-Safety literature. The school will provide parents and carers with information that will assist in keeping children safe online. This will include in 2016 a presentation by an external provider discussing risks and ways to keep children safe online. This presentation will be offered to all parents and carers attending the school. In subsequent years it will focus upon parents and carers of those: in upper Key Stage 2, pupils who have exhibited a weakness in E-Safety understanding (i.e. those children who are willing talk to strangers over Skype or through X-box Live or other forms of online communication) and anyone who joins the school throughout the year.

The Computing Co-ordinator will deliver a fact sheet of "handy-tips" for parents and carers to help keep children safe online, this will include sites and age limits to be aware of and where to look for support in keeping children safe online. This will be distributed once a year to all parents and be available on the school website.

Data Protection:

This section should be read with the Data Protection Policy and is only meant to serve as an outline of data protection in relation to online material.

Western Road CP School makes every effort to ensure that the confidential information in our care is protected. We make every effort to ensure that computing and online technologies are used properly and legally. The following are important legislations that should be considered when dealing with matters of E-Safety and production of work within the learning environment.

Human Rights Act 1998

Article 8 of the Human Rights Act gives everyone the right to respect for their private and family life, their home and their correspondence. The right to private life includes the right to have personal information, such as official records, photographs, letters, diaries and medical information kept private and confidential.

Data Protection Act 1998 (DPA)

This act regulates the handling of personal information relating to living individuals. Personal information includes your:

- name
- contact details
- gender
- ethnicity
- religion
- date of birth
- behaviour
- exam results
- medical history
- offending history.

The DPA requires us to:

- process personal information fairly and lawfully
- only collect personal information we need for specific purposes
- ensure the information is relevant and up to date
- only hold as much information as we need and only for as long as we need it
- keep personal information secure.

The Act also gives people the right to find out what personal information is held about them on computer and most paper records. So it is important that we manage personal information carefully and keep it for the right amount of time. Personal information is kept in locked cabinets in the school office and in password protected parts of SIMS systems only accessible to named users.

The act also provides us with a duty of care not to realise any information to unauthorised body or individual without the proper authority i.e. a non-government agency requesting pupil data. These requests should be made directly to the Headteacher who will consider the merits of the request contacting the LA for advice where they feel it is required.

Computer Misuse Act 1990

The Computer Misuse Act details certain illegal activities, including:

- knowingly using another person's username or password without proper authority
- impersonating another person using email, online chat, web or other services
- misusing authorised access
- using, or helping another person to use, someone else's system for criminal activities
- modifying software or files so as to interfere with the system's operation or to prevent access to or destroy data

- deliberately introducing viruses, worms or other malware to cause a system malfunction.

All staff and pupils are required to sign an acceptable use policy agreement before accessing computers – Appendix 2.

Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act gives the creators of material control over how it is used, whether the material is on paper, film, CD, DVD, websites or databases.

At Western Road CP School we ensure that pupils and staff are aware that:

- all software used within the school must be legally licensed
- material on the internet is protected in the same way as material on other media
- unauthorised use, copying or transmission of copyrighted material is a criminal offence.

Education and Inspections Act 2006

Sections 90 and 91 of the Education and Inspections Act provide statutory powers to schools for disciplining pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 provides a defence for confiscation of inappropriate items from pupils as a disciplinary penalty.

This legislation is important when dealing with E-Safety issues. For example, it gives schools the power to intervene in instances of cyberbullying and to confiscate mobile phones and other personal devices from pupils if they are being used to harm the well-being and safety of others.

Blogging:

This is a proposed policy that maybe fully adopted should the below Focus Group find merit for developing Blogging as part of the school opportunities.

Aims and Objectives:

Whilst blogging has been around for 10+ years, more and more schools are now giving their pupils a voice and an audience through blogging. These are mainly in the form of class blogs but can also be in the form of project blogs (Mantle of the Expert, and others) or individual pupil blogs. Whilst there are many blogging platforms, Wordpress is the most popular. This policy will outline the safe management of setting up and running a blogging platform. A successful blog can:

- Safely give your pupils a wider audience for their learning.
- Encourage reluctant learners to participate and succeed
- Allow pupils to receive feedback safely from many different people
- Allow your pupils to peer assess each other's learning
- Encourage parental engagement
- Provide a platform that can embed Web2.0/3.0 tools into
- Promote your pupils' learning across the globe

E-Safety

Blogging involves pupils working on a blog whilst in school and also at home. To be able to post, pupils need to log into the blog either using an individual sign in or a class sign in. The advantages of individual sign in is that this gives more ownership to each pupil. Most blog platforms allow accounts to have different permissions. Contributor is the lowest level that allows a user to post. A contributor can submit a post for review, however, this will need to be authorised by the admin before it appears on the blog. The 'Contributor' permission level is recommended for Western Road CP School. Any other permission level above that of 'Contributor' will allow posts to be viewable as soon as the pupil clicks 'Submit'.

Should Western Road CP School adopt this policy it will seek permission for each child to have access to a blog, permission to display the learning from each pupil and permission for the photographs of each pupil to be displayed on a blog. **Names will not appear alongside images of pupils** unless additional permission has been sought by the class teacher.

Each pupil with a unique log-in will be reminded to keep this private, if a pupil or parent thinks their log-in needs changing, this can be done in the 'profile' setting on the dashboard. Parents and pupils are to contact the named admin should this need clarifying.

Blog Rules:

Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that you will stay safe whilst blogging.

Don'ts:

1. Never give away any personal information about your location or identity.

2. Don't post pictures of yourself without specific permission from your teacher or parents.

3. Never give out your log-in details to anyone.

4. Don't use text language in your posts

Do's:

1. Post about whatever you like.

2. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.

3. Comment on other people's posts too. Blogging is about commenting and posting!

4. If your post doesn't appear straight away, your teacher might be busy, do be patient.

5. Try to post about things that your audience would like to read.

6. If you see anything that shouldn't be on your screen, **tell your teacher or parents immediately.**

7. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.

8. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.

9. Always tag your posts with your first name and include key words specific to your post.

The Role of the Blog Admin/Teacher:

The blog admin normally is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

1. Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!

2. If you use a shared computer, log out at the end of each session.

3. Promote the links on the class blog to the parents and the wider community. Twitter is a great way to promote a blog.

4. A blog can take a while to gather momentum and an audience. Be patient... the audience will come!

5. Your users will need to log-in. For a quick solution, you can have one Username and Password for your class to get posts on the blog. However, for older pupils of 7+ they are more than capable of having their own log in.

6. The safest permission setting for your blogger is 'Contributor'. This will allow them to log-in and post but the blog admin will need to approve each post.

7. Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!

8. Make sure each blog looks different in your school. This will help keep the interest high for the pupils from year to year.

9. Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.

10. Try using a free project like Quadblogging or Weebly this will give your pupils a quick audience. See http://quadblogging.net or www.weebly.com for more details.

Focus Group:

A focus group will be established comprising of the computing lead, governor and friends of Western Road CP School (FWR). The group will analyse and consider: the impact of the new curriculum on children's learning; how best to assess learners progress; how we can incorporate new and emerging technologies into learning; the development of web based applications that will benefit the continual learning of students to enable them to make a seamless transition to secondary school and be ready for life in the 21st Century. The group will also consider the implication and effect that "blogs" could have on children's (particularly boys) writing.

The SENCO is welcome to take part in these discussions in order to ensure all children's needs are being met.

Appendix 1

Cyber Safety Code

Three Steps to Safety

1. Respect other people - online and off. Don’t spread rumours about people or share their secrets, including phone numbers or passwords.

2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.

3. “Do as you would be done by!” Think how you would feel if you were bullied. You are responsible for your behaviour - so don’t distress other people or encourage others to do so.

If you are being bullied It is never your fault. It can be stopped and it can usually be traced.

- Don’t ignore the bullying. Don’t reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

Text / video messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your number (ask your mobile phone provider).
- Do not reply to abusive or worrying messages. You can report them to you mobile phone provider.

Email

- Never reply to unpleasant or unwanted messages.
- Don’t accept emails or open files from people you don’t know.
- Don’t delete bullying emails – print them or save them as evidence in a separate folder.

Social networking sites, chatrooms and instant messaging

- Change privacy settings so you can choose who to be friends with and who can see your profile. Don’t add anyone you don’t know to your friend list.

- Don’t use your real name in chatrooms.

- Never give out your photo or personal details, like your address, phone number or which school you go to.

- Don’t post any pictures or videos you wouldn’t be happy for your parents or teachers to see. Once they are online they can be copied and posted in other places where you can’t get rid of them.

- Never meet up with strangers, even if they say know people you know or you think they are your friends.

- Keep your passwords private and don’t tell anyone, not even your best friend.

- To report suspicious behaviour online and to learn more about keeping yourself safe online visit www.thinkyouknow.co.uk

Always report bullying incidents. Not doing that allows the bully to continue.

That’s not good for the victims, for those who witness the incidents or for the bully, who may need help to change their anti-social behaviour.

Appendix 2

User Agreements:

Pupil Acceptable Use Policy Agreement – Foundation and KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has 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 adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will use polite language when talking to online.
- I know that if I break the rules I might not be allowed to use a computer.

Child name:……………………………………………

Parent/carer(s)..

Signature(s)..

Pupil Acceptable Use Policy Agreement – KS2

Key Stage 2: Internet Responsibilities

In school, we must use the internet responsibly. When we use the internet at home, we must follow similar rules that we do in school.

- I will act responsibly by following my teachers' and my parents' instructions when using the internet.
- I am responsible for keeping my login and password private.
- I will tell a member of school staff if I think that someone else knows my password.
- I login to accounts using my own username and password ONLY.

Home-School Acceptable Use Policy

- I will use appropriate language when communicating through the internet.
- 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)
- I am responsible for everything that I write on the internet.
- I will only upload, write or share what I want others to see.
- I understand that my teachers will monitor how I use the internet if they receive complaints or suspect that I am using it inappropriately.
- I understand that inappropriate material should not be uploaded or shared through any digital media.
- I will act responsibly by telling my teachers if I think that someone else is behaving irresponsibly by breaking the rules.
- I will check with my teachers or parents before using any website. In school, I use the internet for school work only and with permission from my teacher.
- I am responsible for telling my parents or teachers if I see or read inappropriate material on the internet. If I accidentally see something that upsets me or is inappropriate, I will close the screen before alerting an adult.
- I understand that I must act appropriately when using the school internet and digital equipment at all times.
- I will only bring a mobile phone to school if I need it when walking home without an adult.
- If I do bring a mobile phone it will be handed into the school off turned off for the day.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that if I act inappropriately, my parents/carer will be informed and I will not be allowed access to the school internet for a set period of time (decided by the Headteacher).

Pupil name:

____

Signature:

____

Parent/ carer name(s)

____

Signature(s):

____

* the terms appropriate and inappropriate will be explained to children when discussing this user agreement. Inappropriate will focus on material that is deemed below their age and / or will cause offence or upset individuals or classed as behaviours that do not prompt the school values/rules.

Staff Computer User Agreement

School networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Western Road CP School provides computers, I-Pads, copier equipment and cameras for use by staff. The equipment is provided and maintained for the benefit of all staff in line with the teaching and learning of individuals.

By logging on to or connecting to the school network, you agree to be bound by the conditions of this user agreement. Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Computing Co-ordinator and / or the Headteacher.

Equipment

- Unless you are a designated "privileged" user of a particular workstation, staff users are not permitted to install or attempt to install software onto or uninstall software from any workstation or I-Pad, without the express permission and / or assistance of Schools ICT Services.
- Do not damage, disable or otherwise harm the operation of the computers, or intentionally waste resources. This puts your work and potentially the work of others, at risk.

- Always check files brought in on removable media (CD, USB drives, External hard drives etc) with antivirus software and only use them if they are found clean of viruses. If you are unsure how to do this please check with ICT Schools Services.
- Before connecting your own personal device to the school network you must ensure you have up-to-date antivirus software and relevant major operating system security network. If you are unsure how to do this please contact ICT Schools Services.
- Only school memory cards will be used when taking digital images and permission will be sought from the Headteacher and / or the Computing Co-Coordinator before removing these images from the school premises.
- I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
- I will not use the school network in a way that could disrupt its use for other users.

Security and Privacy

- Protect your work by keeping your password to yourself; use a “strong” password which mixes, upper and lower case letters and numbers, and is at least 8 characters.
- Change your password every 60 days for SIM, Network access and email. You should never use the same password for each school account. When creating a new password, ensure that it is different by at least two characters.
- Never use someone else’s logon name or password – this could be grounds for disciplinary action.
- You will have 3 attempts to enter your password correctly before your account is locked. The Computing Lead will then need to have your password reset.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter settings may put you, your work, or the work of others, at risk, and is forbidden.
- If removing files relating to a child or children then this must only be done on using an encrypted device. The encryption on the device must be active before leaving the premises and should not be shared with non-school personal unless expressed permissions have been sought from the Headteacher or SENCO.
- I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or East Sussex County Council) into disrepute.
- I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.

- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
- Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person.
- I will ensure that I log off after my network session has finished. If I find an unattended machine logged on under other users username I will **not** continuing using the machine – I will log it off immediately.
- I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.

Internet

- I will report any accidental access, receipt of inappropriate materials or filtering breaches / unsuitable websites to the Computing Coordinator.
- I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
- I will not accept invitations from children and young people who add me as a friend to their social networking sites, nor will I invite them to be friends on mine. For further guidance on this matter please reference pages 8 and 22 of the ‘Staff Handbook September 2015’.
- As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children. I will regularly review my security settings of social media sites to ensure they have not changed my visibility settings without my knowledge.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role in any way. Please see the ‘Staff Handbook September 2015’, pages 8 and 22, for further guidance on this matter.
- Activities such as buying or selling goods are permitted within reason, provided the process does not impinge on school business. Note that the school and / or its computers does not accept liability for credit card fraud or other criminal practices if a workstation is used for personal business.
- If you intend to download large amounts of data on your school laptop, such as files from a portable music player or digital images or from your cloud

server, you must inform the Computing Coordinator who will advise you where this data should be stored. If you store large amounts of this sort of data without informing the Computing Coordinator it may be deleted without warning.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is considered anti-social behaviour.
- Only open attachments to emails if they come from someone you know and / or trust. Attachments can contain viruses or other programs that could destroy files or software on the workstation and / or network/
- The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden. This includes material of a violent, dangerous, racist, or inappropriate content.

General

- All staff are expected to have a digital image of their likeness included on the website and VLE unless agreed otherwise with the Headteacher.
- I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
- I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on the SIMS Learning Gateway.
- I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
- I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
- Staff must comply with the acceptable use policy of any other networks that they access.
- All staff must be aware of the Computing, E-Safety and Cyberbullying Policy 2015/16 for requirements in addition to this user agreement.
- There will be no warranties of any kind, whether expressed or implied, for the network service offered by the Western Road CP School. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

- Users are expected to inform Computing Coordinator immediately if a security problem is identified and should not demonstrate this problem to other users. Any users identified as a security risk will be denied access to the network.

If you violate these provisions, access to the network may be denied and you may be subject to disciplinary action. Additional action may be taken by Western Road CP School in line with existing policies regarding staff behaviour. Where, appropriate, the police may be involved or other legal action taken.

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Computing Coordinator.

I agree to report any misuse of the network to Computing Coordinator.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to Computing Coordinator.

Lastly, I agree to ensure that portable equipment such as cameras, laptops or I-Pads will be kept secured when not in use and to report any lapses in physical security to Computing Coordinator.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: ____

Staff Signature:__________________________________ Date: _ _ /_ _ /_ _ _ _

Appendix 3

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/E-Safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the Computing Co-ordinator and ensure the site is filtered by reporting to ICT Schools Services.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform ICT School Services and ensure the site is filtered if need be.

An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the ICT School Services and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
    a. Contact the local police and follow their advice.

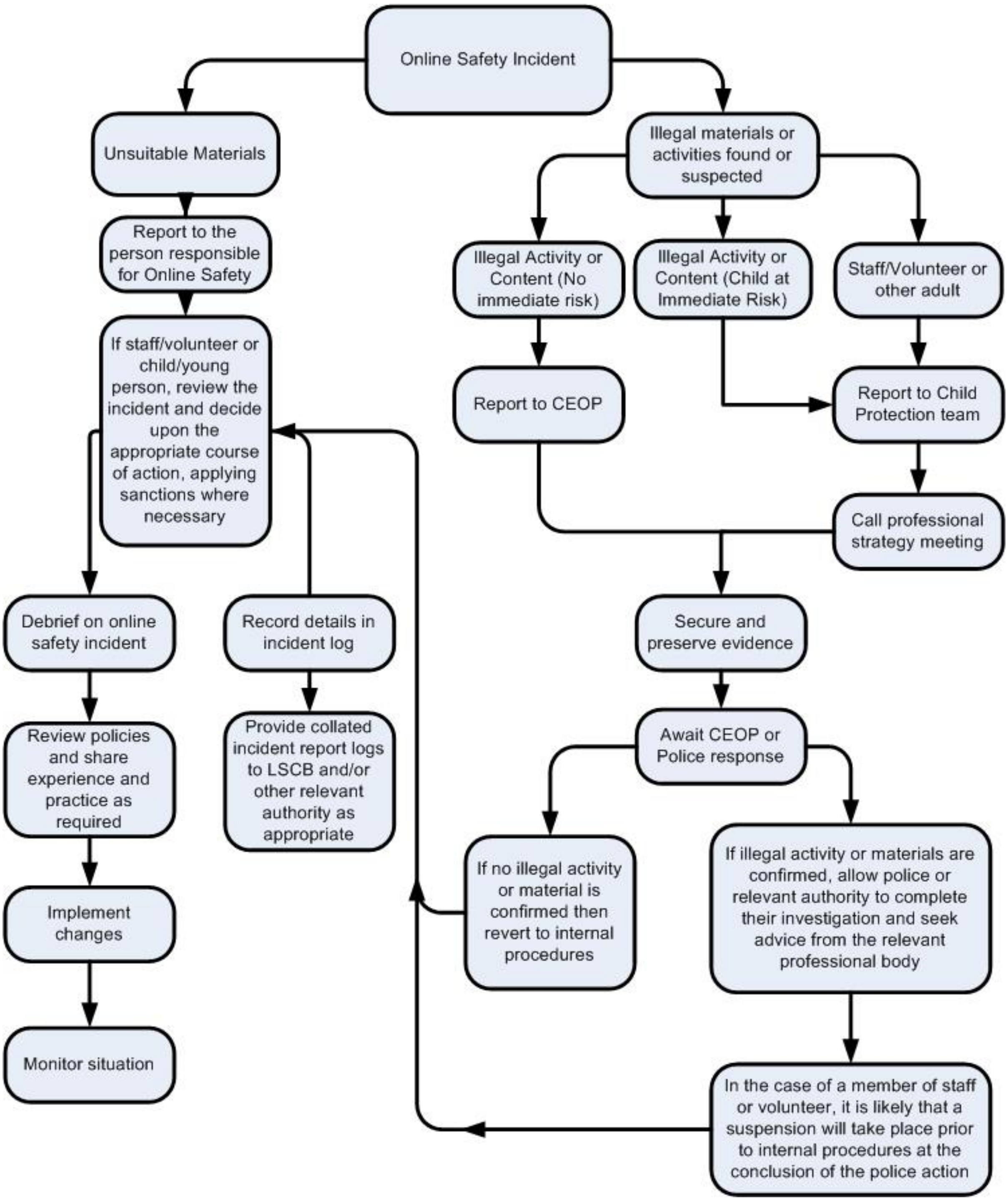
An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Headteacher and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the Headteacher should then:
    - Remove the device to a secure place.
    - Instigate an audit of all computing equipment by ICT Schools Services to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (undertaken by Headteacher).
    - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
    - Contact the local police and follow their advice.
    - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the Headteacher and E-Safety officer.

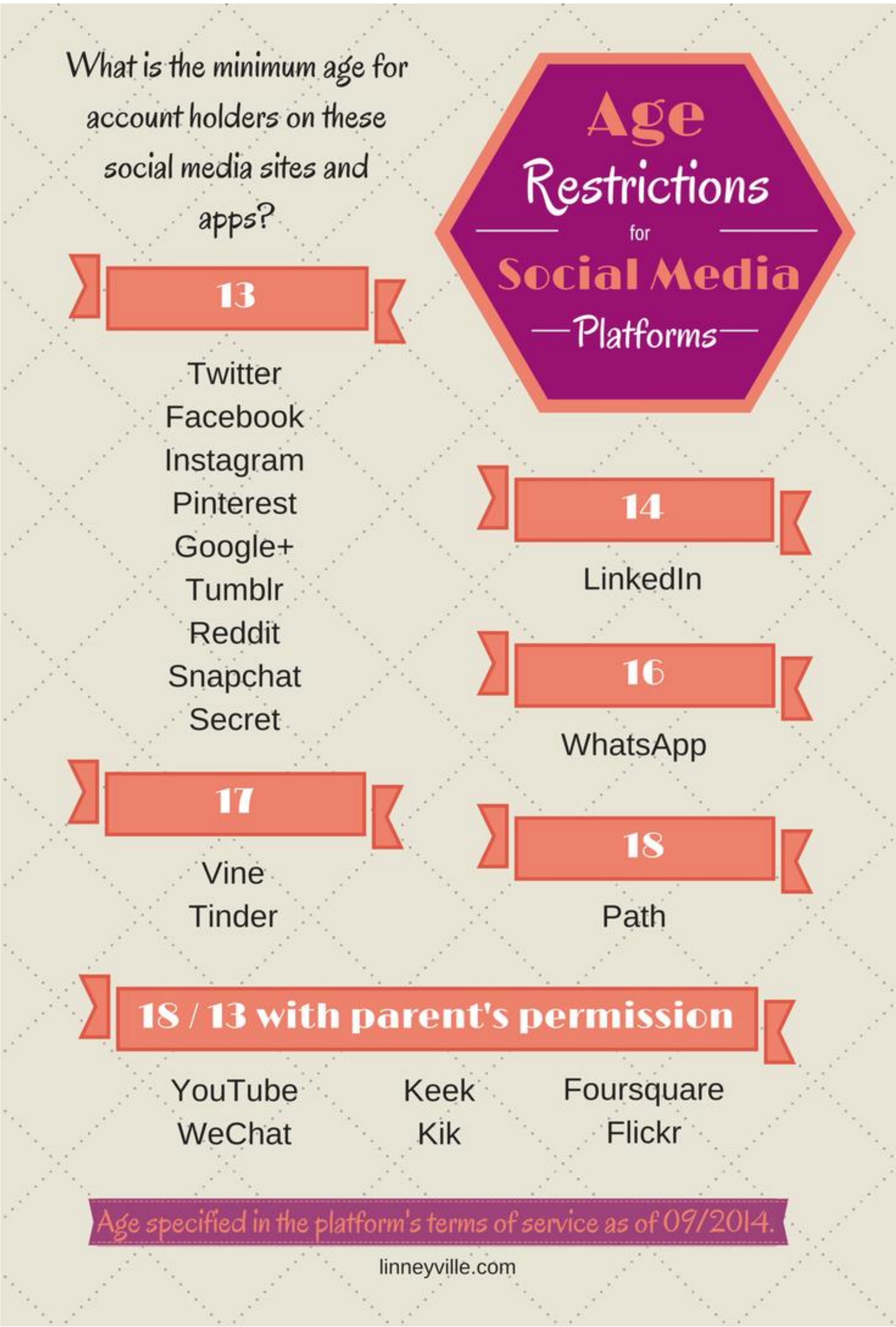
Appendix 4

Responding to incidents of misuse – flow chart



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

Appendix 5



Age Restrictions for Social Media Platforms

What is the minimum age for account holders on these social media sites and apps?

13

Twitter
Facebook
Instagram
Pinterest
Google+
Tumblr
Reddit
Snapchat
Secret

14

LinkedIn

16

WhatsApp

17

Vine
Tinder

18

Path

18 / 13 with parent's permission

YouTube	Keek	Foursquare
WeChat	Kik	Flickr

Age specified in the platform's terms of service as of 09/2014.

linneyville.com

Glossary

Internet – the physical hardware that allows access to the World-Wide-Web.

Website – A page of information stored digitally on the Internet. (Think of a webpage as if it is a memory stored in the brain and the Internet is the physical place where these memories are stored).

Blogging – A blog is a web-based self-publication made-up of periodic articles/ Blogs use post-based entries catalogued by time and date.

RSS – an acronym for Really Simple Syndication. It is a family of XML file formats for web syndication used by news websites, podcasts, vblogs and audioblogs. The technology behind RSS allows you to subscribe to websites that have provided RSS feeds. These are typically sites that change or add content regularly. To use this technology you need to set up some type of aggregation service using aggregator software.

Aggregator – An aggregator, is software application, webpage or service that automatically collects updated publications from a number of sources, such as RSS and other XML feeds from blog, audioblog or vblog websites that the user has signed up to.

Audio-blogging – is a variant on blogging using audio to reach the audience instead of text used by traditional blogs. Audio-blogs have a similar form as blogs. There is usually a title and brief description, but the bulk of content is in the linked audio file.

Vblogging – A vblog (short for video-blogging) is a blog that uses videos as the primary content. Vblogs are usually accompanied by supporting text to provide a context for the video.

Podcasting – is a method of publishing audio broadcasts via the Internet, allowing users to subscribe to a feed of new files (usually MP3s). Podcasting is distinct from other types of online media delivery because of its use of subscription websites.

Moblogging – is a term to describe groups of people using mobile phones to create and share podcasts on a common subject.

Bluejacking – the sending of anonymous text messages over short distances using Bluetooth wireless technology.

Netiquette – the polite and socially acceptable way to behave online.

Sexting – sending or receiving digital images of a sexual nature via any digital platform or device.

http://www.internetmatters.org/schools/primary/