Exe Valley Federation
CHALLENGE DISCOVER SUCCEED

E Safety Policy

Date of publication: November 2020 Review date: Autumn 2023

Core purpose statement
In a creative, caring environment, we all support and challenge each other to develop confidence and independence. As active global citizens, we are inspired to discover and succeed in lifelong learning.

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

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole federation community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable risk of harm to the child or liability to the federation.

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 sites 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 schools, but is linked to membership of the schools or federation. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the federation Behaviour Policy.

The federation 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
The following section outlines the E-Safety roles and responsibilities of individuals and groups within the federation:

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 Full Governing Board who will undertake:

- regular meetings with the ICT Technician
- regular monitoring of any e-safety incidents
- reporting to relevant Governors meetings

Executive Headteacher [EHT] and Federation Leadership Team:

- The EHT has a duty of care for ensuring the safety (including E-Safety) of members of the federation community, although the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator.
- The EHT and at least one another member of the Federation 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 flow chart on dealing with E-Safety incidents – included later – "Responding to incidents of misuse"at Appendix 4 and "What we do if" Appendix 2

- The EHT and Heads of School are responsible for ensuring that the E-Safety Co-ordinator 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 EHT and Heads of School 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-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Federation Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Co-ordinator (ICT Technician)

The E-Safety Co-ordinator is the ICT Technician. He is managed by a Head of School and liaises with the ICT Service Provider to undertake the following duties:

- take day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the federation E-Safety policies and documents;
- ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place;
- undertake an annual audit of staff training needs for discussion with Governors
- provide training and advice for staff;
- ensure ICT Incidents are logged

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current federation E-Safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy at Appendix 3
- they report any suspected misuse or problem to the Head of School and E-Safety Technician for investigation and action;
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using recognised 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.

Designated Safeguarding Lead

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 on-line contact with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy shown at Appendix 3A 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 cyber-bullying;
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the federation's E-Safety 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 federation will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local E-Safety campaigns and literature. Parents and carers will be encouraged to support the federation in promoting good E-Safety 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 and
- their children's personal devices in the school (where this is allowed).
- Parents are requested to sign the permission form at Appendix 3 to show their support of the school in this important aspect of the school's work.

Teaching and Learning

Use of the Internet

The federation recognises that the Internet is an essential element in 21st century life for education, business and social interaction. The federation has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DfE.
- access to learning wherever and whenever convenient.

Using the Internet to Enhance Learning

- The School Internet access will be designed expressly for educational use and the purposes of running the school and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating Internet Content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and

pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Internet Access

Internet access will be supervised and children will be encouraged to used previously vetted websites. Children will be taught how to use safely a variety of search engines and be taught specific skills in locating information effectively using search engines. Pupils will sign the acceptable use policy and these will be sent home to parents with an accompanying letter to support parents in keeping their children safe when using the Internet at home.

Acceptable Use of Internet Statements

The computer system is owned by the federation and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and engagement. The federation's 'Acceptable Use Policy' has been drawn up to protect all parties - the pupils, the staff and the federation. The federation reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

Managing Communication

E Mail

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Pupils and staff should be aware that school email may be monitored.
- All staff will have access to work email addresses which will form an integral part of communication within the school.
- If accessing emails from a mobile or personal laptop staff will not link their work email accounts to an app but sign in through the appropriate email platform.
- Personal email accounts may only be used during school breaktimes.
- All email (both incoming and outgoing) is checked for banned words and for viruses. Any breach of content is reported and dealt with.

Mobile Phones

- It is inappropriate for children or parents to contact members of staff on their mobile phone.
- Mobile phones will not be used during lessons or formal school time. Mobile phones should not be used in the corridors or in learning areas during the school day. The sending of abusive or inappropriate text messages is unacceptable.
- Children will not use mobile phones in school. If they bring a phone to school, because they need it when walking home, they must keep it secure and kept away during school hours. Children should hand any mobile phones to teachers before going on the visits as they are not needed on school visits.
- Staff and parents should not use cameras and videos on mobile phones to record images or videos whilst on school visits.

Use of Digital and Video Images

The use of cameras and video is an essential and integral part of everyday life. Staff and children should be encouraged to use this technology in a positive and responsible way. For details see Appendix 1.
This policy complies with the requirements of the Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998 and other relevant Acts regarding the taking and use of photographic images of children. The Federation Leadership Team is responsible for ensuring the acceptable, safe use and storage of camera technology and images.

Published Content

The School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupils' Images or Work

- Images that include pupils will be selected carefully and only published when parental approval has been given [see bullet point below].
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parents or carers are asked to return a signed form if they do not wish images of their children to be used electronically.

Managing Social Networking and Personal Publishing in School

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or his/her location e.g. house number, street name or school.
- Staff must not run social network spaces for pupils' use on a personal basis.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Pupils will be shown how to publish and present information to a wider audience.

Social Networking - Staff

- Staff are advised to be cautious of information shared on social network sites and be mindful of who has access to this information and the importance of good privacy settings. Anything said, shown or received could be made available to a wider audience than originally intended. (Facebook "Friends only" / be aware that all tweets can be accessed by the general public unless you specifically change your account to a private one.)
- Check what can be accessed on your profile – it could be your contact details and photos people have posted.
- Federation staff must not disclose, on any social networking site, any information that is confidential to the Federation, Governing Body, or Local Authority; or post anything that could potentially bring the Federation, Governing Body or Local Authority into disrepute. Think about the content of what you write and of the photographs published. Ask yourself, if you would feel comfortable about a current or prospective employer, colleague, pupil or parent, viewing your content.

- Social networking sites create a written record of what you write which can be used in disciplinary action if it is used unprofessionally or inappropriately.
- Employees and individuals otherwise engaged by the federation are not permitted to access social networking sites for personal use via school information systems or school equipment at any time.
- All members of the federation community must be conscious at all times of the need to keep their personal and professional lives separate. Staff should not be friends or share information with pupils. Keep a professional distance from parents at the school.
- If staff have any concerns about the use of social networking sites in relation to school please speak to a member of the Federation Leadership Team.
- When using social media on behalf of the school or federation (e.g. on Twitter), staff must follow the guidelines in Appendix 5 'Guidelines when Posting on behalf of the School'

Advice from teaching unions include:

- Be sensible and mind your language! Don't make negative or inappropriate comments about your colleagues, pupils or school.
- Don't be friends with pupils on Facebook. Keep a professional distance at all times.
- Don't appear in inappropriate photos.
- Increase the privacy settings for your own profile.

Managing Filtering

- The federation will work with the Broadband provider (currently SWGfL) to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Technician
- The ICT Technician will liaise with the Broadband provider to ensure filtering is effective and appropriate
- Any material that the school believes is illegal must be reported to the Head Teacher who will report it to appropriate agencies such as IWF or CEOP.

Managing Information Systems

Security & Protecting Personal Data

- The security of the federation information systems will be reviewed regularly in accordance with the SLA with the Internet Service Provider.
- Virus protection will be updated regularly.
- Sensitive personal data sent over the Internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

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 Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the federation 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 federation audits ICT 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.

Handling E Safety Complaints

- Complaints of Internet misuse will be dealt with by a member of the FLT.
- Any complaint about staff misuse must be referred to a member of the FLT
- Parents and pupils will need to work in partnership with staff to resolve issues.

Implementing this Policy

All users below will be expected to complete an Acceptable use policy. This will be re-distributed in September 2022, thus also ensuring a record of who has completed this is kept. The text of these policies is show at Appendix 3 a,b,c,d

With children

- E-Safety rules are posted in classrooms.
- Pupils are informed that network and Internet use will be monitored.
- The federation incorporates e-safety learning into ICT learning to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use of the Internet is an integral part of ICT learning in school.

With staff

- All staff have access to the Federation e-Safety Policy and its application and importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff training in safe and responsible Internet use and on the federation e-Safety Policy will be provided as required.

With Parents / Carers

- Parents' attention will be drawn to the federation's e-Safety Policy in newsletters, the school brochures and on the school websites.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart at Appendix 4 for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the federation community will be responsible users of digital technologies, who understand and follow federation policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. See Appendix 2 which outlines **"*What we do if..*"**

Review and monitoring

Each year an audit will be undertaken of the effectiveness of the federation's adherence to this E- Safety Policy.
Policy to be reviewed annually or before 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.

Policy Date: June 2017
Last Review Date: October 2021
Last Review Conducted By: Dave Alcock/Sophie Dunn
Agreed by Full Governors: 12th October 2021
Review date: Autumn 2023

Accepted Differences

- Updated terminology, personnel and current usage
- Updated roles and responsibilities
- Additional section re accessing emails from a mobile or personal laptop staff will not link their work email accounts to an app, but sign in through the appropriate email platform

Authorisation
The above differences have been approved.

Signed.....Chair.

Date:.....

Appendix 1: Images and Video

For the purposes of this guidance, an image is a still or moving picture of a person who can be identified.

When a school captures a person's image, whether it is by camera, CCTV, video, web camera or mobile phone, and that person can be identified, then the image is likely to be considered personal data. This means that the image must be processed in line with the data protection principles. 'Processing' means anything that is done to the image for example recording it, using it or sharing it.

At Exe Valley Federation schools we do not allow parents to take video and photographs at school events because some children are not allowed to have their images shared on the internet. We issue parents with a copy of our e-Safety Policy which sets out what we do with digital images:

- 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.
- Staff 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 only be used in exceptional circumstances such as on residential and this use must be agreed, in advance, with the EHT or E-Safety Technician.
- Pupils must not take, use, share, publish or distribute images of others, taken in school, 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 the school website or public pages.
- Parents have the right to refuse permission for the school to publish their child's photo or video image on the school website or in local media and should notify the school, in writing, if they do not want their child's photo published. The school will work from the premise that parents/carers are happy for their child's picture to be published.

  Parents are asked to inform the school if they do not wish their child's image to be used or shared as outlined above

Appendix 2: Guidance: What do we do if?

An inappropriate website is accessed <u>unintentionally</u> 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 ICT Technician and ensure the site is filtered by reporting to SWGfL

An inappropriate website is accessed <u>intentionally</u> 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 the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> 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 school technicians and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA/RBC.
6. In an extreme case where the material is of an illegal nature: 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 Head of School (or named proxy) 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 Head of School should then:
   - Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by the school's ICT managed service providers or technical teams 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 Executive 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 Executive Headteacher and e-safety officer.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message and to retain it for evidence.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.

8. Inform other agencies if required (LA, Child protection,)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Head Teacher

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Appendix 3A: Pupil Acceptable Use Policy (KS2)

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

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 may 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 a trusted 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 (e.g. YouTube), unless I have permission of a member of staff to do so.

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 have permission to 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, 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.

Name of Child / Pupil	
Class	
Signed [child]	
Date	

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

Signed (child):……

Use of Cloud Systems Permission Form [to be used when needed]

The school uses [name of cloud system] for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil and hosted by Google as part of the school's online presence in [name of cloud system]:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of pupil use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a [name of cloud system] account:

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above pupil, I agree to my child using the school using [name of cloud system]. Yes / No

Signed	
Date	

Staff (and Volunteer) Acceptable Use Policy

Federation 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 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 federation 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
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 children / 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 may 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, Virtual Learning Environment 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.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and the permission of their parents 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, and these images will be deleted from my personal equipment and any other personal storage devices these are saved to (including automatic cloud e.g. Dropbox, Flickr, Google+). Where these images are published (e.g. on the

school website / Virtual Learning Environment) 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.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- 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 or on personal devices other than at break times.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School 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).

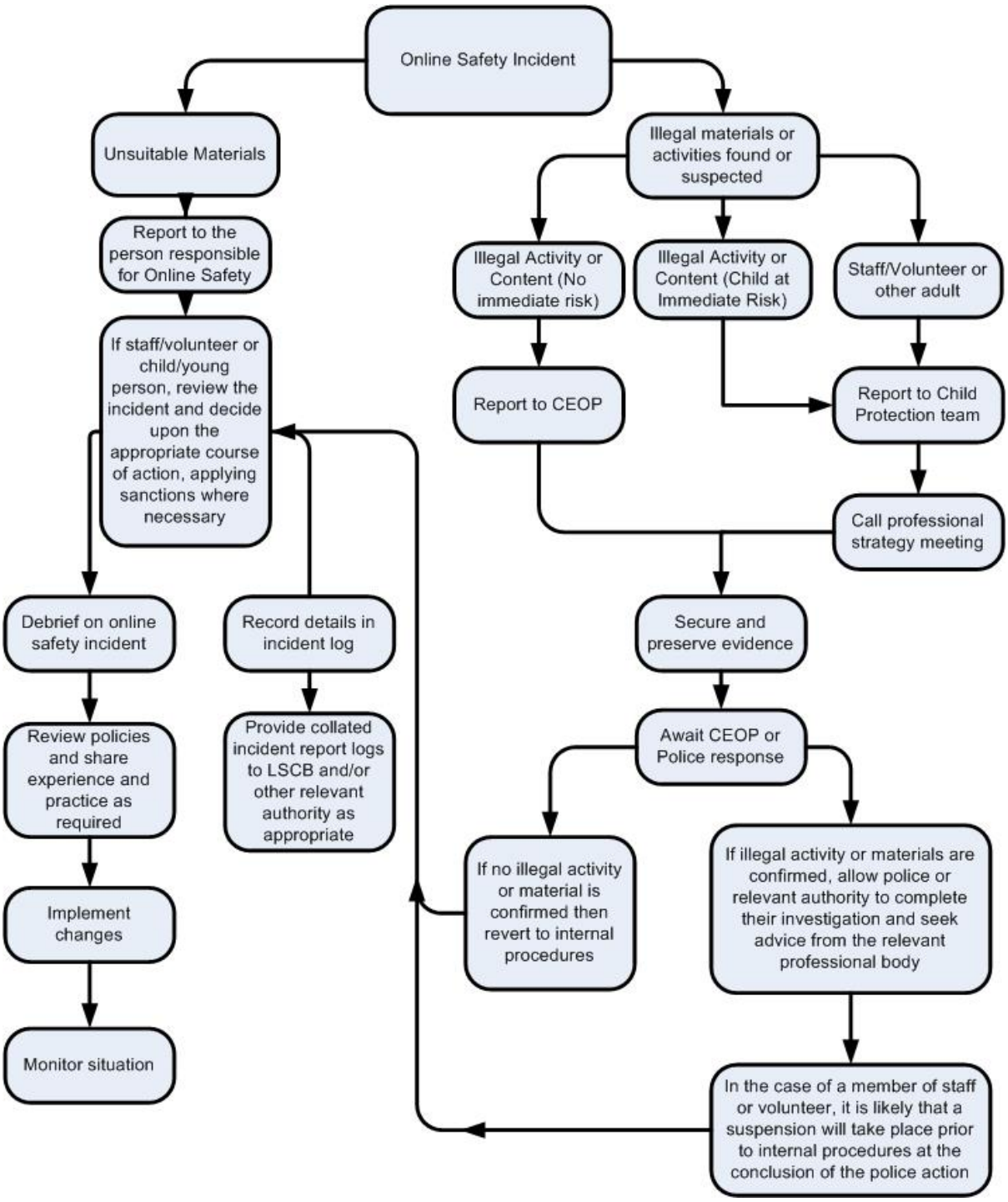
I understand that I am responsible for my actions in and out of the school:

- 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 / academy
- I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the federation's E-Safety Policy 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	

Responding to incidents of misuse – flow chart



Guidelines when posting information online on behalf of the federation

Aims of Using Social Media on behalf of the Federation:

- To quickly share and celebrate children's achievements, successes and school updates.
- To demonstrate safe and responsible use of social media
- To encourage the use of 21st Century technology

Guidelines

- The relevant school account, website or blog will be monitored by a member of the FLT
- Senior leaders will monitor "followers" and block any who appear to not be school focused.
- The school social media accounts, on Twitter for example, will only follow educationally relevant accounts;
- Users of the school social media account should be careful when responding to any 'replies'; this is not the platform to discuss or debate school related issues.
- Users of the school social media accounts and pages will not use individual children's full names when referencing them.
- The school uses social media sites to share positive messages and information about the school.
- The school may use photos of children's faces as long as permission has not been refused. Any photos posted will be in relation to work and learning. For example, we may share a photo of a child creating a piece of artwork or playing sport.
- The account may be used to share news and information during a school trip. The account will be run by a senior teacher on a mobile device for the period of the trip. Photos taken on the device for the purpose of sharing on social media will be deleted once they have been shared.
- Individually targeted content will not be posted e.g. "Well done Josh a better lesson today". For example, tweets to a year group or class along the lines of "don't forget the..." are acceptable. Although always think about the most effective way to communicate important information.
- By endorsing the use of social media, we may be encouraging children to use it themselves so reinforce e-safety rules such as : "Never post anything that would be potentially upsetting; make sure you know how to report to anything you find that disturbs you; be careful who you talk to they may not be all they appear; never meet anyone from the online world without telling your parents."