The Forest CE Federation

Computing Policy

Visions and Aims

The Forest CE Federation aims to provide children with an exciting, broad and balanced curriculum that will instil a love of learning. Our approach enables all children to become lifelong learners by developing transferable skills to equip them to succeed in a competitive world. A strong **Christian** ethos permeates through our daily lives ensuring our pupils are cared for in a safe, nurturing environment within our small **community.**

Everyone is valued as an individual and helped to develop and progress in their own unique way within a Christian environment. Our vision**, 'Small enough to care, Large enough to inspire , Valuing All God's children'** is at the core of everything we do. The curriculum we offer is not merely academic, but embraces the spiritual, moral, social and cultural development of all pupils and is deeply rooted in our vision that:

 'All things are possible for one who believes' Mark 9 v23 .

We believe in the "whole child" and are committed to children's wider well-being through our **creative** inclusive curriculum, which is driven by our spiritual values.

Our curriculum is designed to spark **curiosity** in young minds through carefully planned opportunities for pupils to acquire, apply and master their knowledge and skills in a unique learning environment.

We know that a child who feels happy, safe and secure will have the **confidence** to try their best and achieve in all that they do. We endeavour to provide all children with the knowledge, skills and environment in which to thrive.

Our curriculum is underpinned by two main threads :

- **For ALL our children to develop high levels of oracy. To have a rich and broad vocabulary, to be confident and literate within society.**

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **To know about the world: to know what it has to offer, how it differs from their locality and how others experience the world.**

We define progress as the widening and deepening of essential knowledge, skills, understanding and behaviours. This is done through how we deliver our curriculum: Continuous Provision

Development / Monitoring / Review of this Policy

This policy has been developed by a working group made up of:

- Headteacher
- School Online Safety Offier
- NCC Online Safety Officer – Simon Aston
- Staff – including Teachers, Support Staff
- Governors

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by the:	Senior Leadership Team Online Safety Co-ordinator School Leads
Monitoring will take place at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2023

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Should serious online safety incidents take place, the following external persons / agencies should be informed:	Safeguarding Governor – John Brough NCC Online Safety Officer LADO/MASH

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students/ pupils
    - parents / carers
    - staff

Scope of the Policy

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

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

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section –

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

"Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).

- The Headteacher is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering
- attends relevant meeting Governors
- reports regularly to Senior Leadership Team

Technical staff

Technical Staff / Co-ordinator for Computing is responsible for ensuring:

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required online safety technical requirements and any Local Authority Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation
- that monitoring systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current school / academy Online Safety Policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy**
- **they report any suspected misuse or problem to the Headteacher for investigation**
- **all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems**
- online safety issues are embedded in all aspects of the curriculum and other activities

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

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

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Pupils:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online 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 school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school / academy (where this is allowed)

Policy Statements

Education – Pupils

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

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

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

- **A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- 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

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

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

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

- Curriculum activities
- Parents / Carers sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/   http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Officer will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association
- Participation in school training / information sessions for staff or parents

Technical –equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- The administrator passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. **Personal data cannot be**

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

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

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

- **Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- 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 not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- **It has a Data Protection Policy.**
- **It has appointed a Data Protection Officer (DPO).**
- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.**
- **The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.**
- **Data Protection Impact Assessments (DPIA) are carried out.**
- **It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.**
- **Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.**
- **There are clear and understood data retention policies and routines for the deletion and disposal of data.**
- **There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.**
- **Consideration has been given to the protection of personal data when accessed using any remote access solutions.**
- **All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **All staff receive data handling awareness / data protection training and are made aware of their responsibilities.**

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

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

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

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.   Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school / when using school equipment or systems. The school policy restricts usage as follows:

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, productionor distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)						
On-line gaming (non-educational)						
On-line gambling						
On-line shopping / commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting e.g. Youtube						

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(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 (below and appendix) for responding to online safety incidents and report immediately to the police.

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at Immediate Risk)

Staff/Volunteer or other adult

Report to CEOP

Report to Child Protection team

Call professional strategy meeting

Secure and preserve evidence

Await CEOP or Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - o   incidents of 'grooming' behaviour
    - o   the sending of obscene materials to a child
    - o   adult material which potentially breaches the Obscene Publications Act
    - o   criminally racist material
    - o   promotion of terrorism or extremism
    - o   other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:
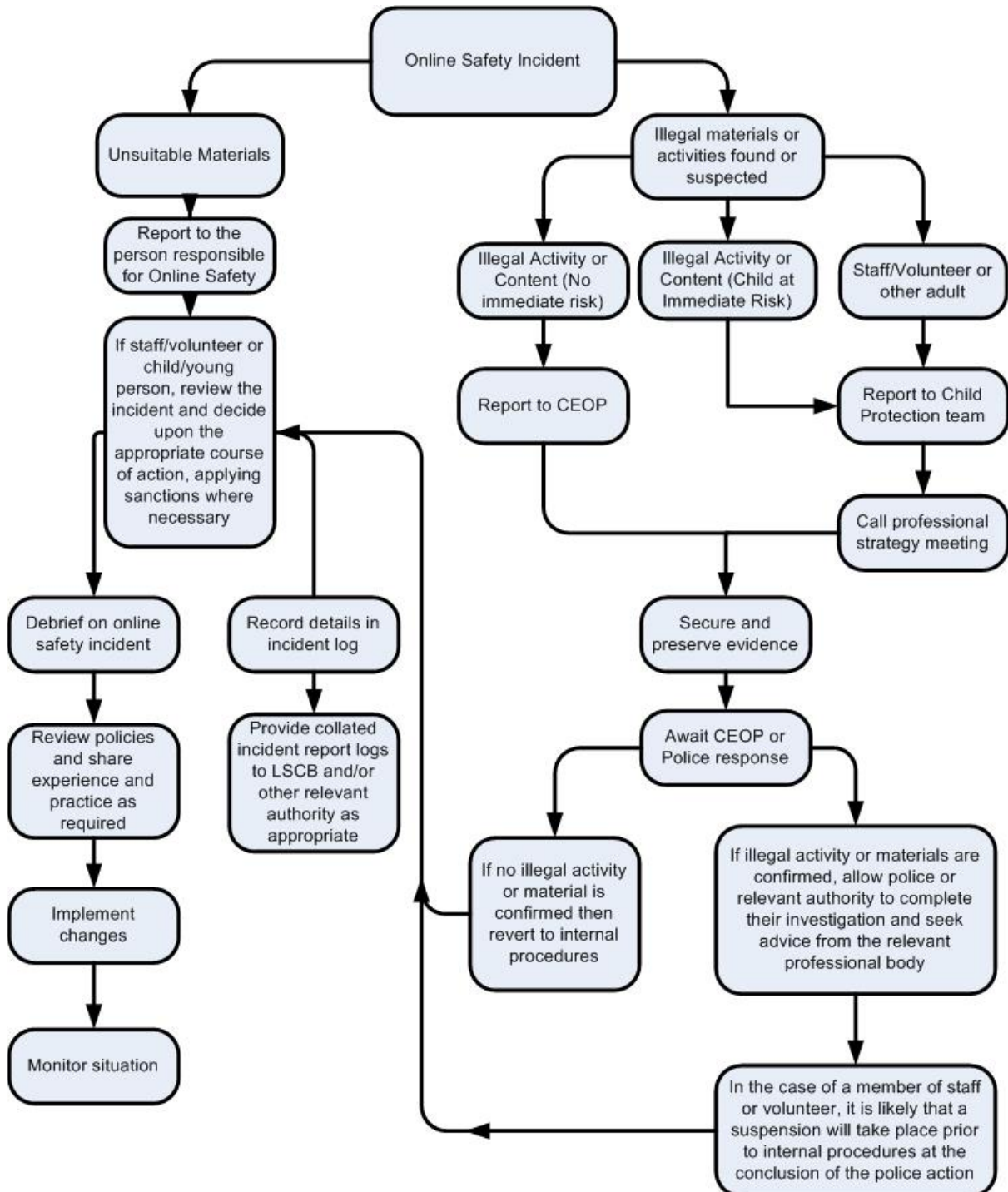
The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Actions / Sanctions

Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year /	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access	Warning	Further sanction eg detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons									
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device									
Unauthorised / inappropriate use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Allowing others to access school / academy network by sharing username and passwords										
Attempting to access or accessing the school / academy network, using another student's / pupil's account										
Attempting to access or accessing the school / academy network, using the account of a member of staff										
Corrupting or destroying the data of other users										
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature										
Continued infringements of the above, following previous warnings or sanctions										
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school										
Using proxy sites or other means to subvert the school's / academy's filtering system										
Accidentally accessing offensive or pornographic material and failing to report the incident										

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Deliberately accessing or trying to access offensive or pornographic material								
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23

Careless use of personal data e.g. holding or transferring data in an insecure manner									
Deliberate actions to breach data protection or network security rules									
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils									
Actions which could compromise the staff member's professional standing									
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy									
Using proxy sites or other means to subvert the school's / academy's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Breaching copyright or licensing regulations									
Continued infringements of the above, following previous warnings or sanctions									

The Forest CE Federation

'Small enough to care. Large enough to inspire

Valuing all God's children '

'All things are possible for one who believes' Mark 9 v 23