Calow Church of England (VC) Primary School

Online Safety Policy

This policy has a child friendly version that has been put together by the Online Safety Group.

Rationale

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

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of our wider duty of care to which all who work in this school are bound. Our school Online Safety policy will help to ensure safe and appropriate use. The development and implementation of this policy will involve all the stakeholders in a child's education from the head teacher and governors to the leadership team and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home have been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The increased risk of online radicalisation from terrorist and extremist material.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which

they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school demonstrates that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This Online Safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but which are 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 school's Behaviour Policy.

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

Roles and Responsibilities

Governors: Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. They will also be involved in monitoring provision and effectiveness of Online Safety through reports given to the Full Governing Body and through the Link Governor process. They will ensure that Online Safety incidents have been dealt with appropriately and that the policy is effective in managing those incidents.

The Safeguarding Governor (Mrs S. Cotton) has overall responsibility for governance of Online Safety. The Safeguarding Governor will have the responsibility for keeping up to date with emerging risks and threats through technology use; will receive regular updates in regards to training, identified risks and any incident logs and will attend meetings of the School Council Online Safety Group.

Headteacher and Leadership team: The Head teacher (who is also Designated Safeguarding Lead) is responsible 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 Lead (who is also the Assistant Head and Computing Lead).

The Head teacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

The Head teacher and 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.

Online Safety Lead:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents. a programme of training and awareness.
- leads the School Council Online Safety Group
- is responsible for recommending resources for staff and pupils to use
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- ensures that the use of the network / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation / action / sanction.
- provides training and advice for staff.
- liaises with the Local Authority on Online Safety matters.
- liaises with school ICT technician on Online Safety matters, including internet filtering and monitoring.
- receives reports of Online Safety incidents and creates a log of incidents to inform future developments.
- meets regularly with the Computing Link Governor / Safeguarding Governor to discuss current issues, review any incident and discuss any Online Safety developments.
- advises the Headteacher and Governing Body on Online Safety matters.
- reports regularly to the Leadership Team.

ICT Technician:

The school has a contract with Derbyshire County Council for the maintenance of its ICT infrastructure. Any person contracted by the school to provide technical services will ensure that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- anti-virus is fit for purpose, up to date and applied to all capable devices.
- that any monitoring software / systems are implemented and updated as and when agreed in school.
- they act within the Online Safety technical requirements outlined in the relevant Local Authority Online Safety Policy and guidance.
- users may only access areas of the school's network appropriate to their role.
- the administrator password is changed on a regular basis.
- web filtering is checked on a regular basis.
- the web filtering host is informed of issues relating to the filtering applied.
- they keep up to date with Online Safety technical information in order to effectively carry out their role and to inform the Online Safety Lead and Headteacher of any concerns regarding Online Safety.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

• They have an up to date awareness of Online Safety matters, including the risk of online radicalisation, and of the current school Online Safety policy and practices.
• They have read, understood and signed the school Staff Acceptable Use Policy
• They report any suspected misuse or problem to the Online Safety Lead /Head teacher for investigation / action / sanction
• Digital communications with pupils (Learning Platform) should be on a professional level and only carried out using official school systems.
• Digital communication with parents / carers should be on a professional level and only carried out using school systems.
• Online Safety issues are embedded in all aspects of the curriculum and other school activities.
• Pupils understand and follow the school Online Safety and Acceptable Use Policy.
• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• They monitor Computing activity in lessons, extra-curricular and extended school activities.

• They are aware of Online Safety issues related to the use of digital technology, including portable devices and that they monitor their use and implement current school 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.
• Any Online Safety incident is reported to the Online Safety Lead, Designated Safeguarding Leads or Headteacher.
• They bring to the attention of the Headteacher any further training in this area that they feel they require.

Designated Safeguarding Lead
The Designated Safeguarding Lead should have up-to-date knowledge about online safety issues and be aware of the potential for serious child protection issues to arise from:
- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- The increased risk of online radicalisation from terrorist and extremist material.

Online Safety Group
The Online Safety Group involves pupils and Governors in decision making, on-going review of policy and procedures, communication and further development of Online Safety in school.

Pupils:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding (at an age appropriate level) of research skills, creative commons licensing 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of digital technologies than their children. The school will therefore take every opportunity to help parents understand these issues through parents' information evenings, high profile events, such as Safer Internet Day, newsletters, letters, website / Facebook and reference to relevant websites / publications.

Parents and carers will be responsible for:
- endorsing (by signature) the Pupil Acceptable Use Policy.
- accessing the school website and Facebook Page in accordance with the relevant school Acceptable Use Policy.

Community Users
Community Users who access school digital technology systems as part of any extended school provision will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

Teaching and Learning

Calow Church of England (VC) Primary School understands that 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.

Online Safety education will be provided in the following ways:

- An Online Safety programme is provided as part of Computing / PHSE / other lessons and is regularly revisited – this covers both the use of digital and new technologies in school and outside school and is age appropriate. This is based on the South West Grid for Learning's Digital Literacy Scheme of Work.
- 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 helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of digital technologies, the internet and mobile devices both within and outside school.
- 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 being provided with a safe environment for learning about controversial issues and by helping them to understand how they can influence and participate in decision-making.
- Rules for use of digital technology systems / internet will be posted in all rooms
- Staff should act as good role models in their use of digital technology, the internet and mobile devices.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of digital technology across the curriculum.

All children are taught how to work safely on the computers and, more specifically, online throughout their time at Calow C of E Primary School. The methods, information given and resources used are at an age appropriate level and strive to encourage safe and responsible use of digital technologies both in and out of school. Aspects of Online Safety should be included in each term's planning and through Anti-bullying week as well as when specific issues arise within class. Children are aware of the 'Rules of Responsible Internet Use' which are displayed in the Computing Suite and classrooms and know that a breach of these rules will be acted upon in a manner consistent with the school's Behaviour Policy and Code of Conduct.

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 use the Internet, especially through search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Pupils should always be made aware by staff that searching for images on a search engine, for example, Google Images, Bing etc. is unacceptable in school.

Training

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.

- 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.
- The Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Online Safety Policy and its updated will be presented to and discussed by staff in staff meetings and Governors in Governors' meetings.
- Governors should take part in online safety training, with the Safeguarding Governor having a higher level of training. This training may be provided by external agencies, the Local Authority or through school.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / 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:

- 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.
- All users (at KS2 and above) will be provided with a username and secure password by their Class teacher (through the Online Safety Lead and ICT technician) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and Online Safety Lead and kept in a secure place (eg school / academy safe).
- The School Business Officer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Any requests for filtering changes must be agreed by the Headteacher.
- Internet filtering is in place to ensure that children are safe from terrorist and extremist material when accessing the internet.
- Pupils and staff are aware of the procedures for reporting a breach in filtering. (See Safe Surfing of the Internet below).
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. They are given temporary passwords which allow varying levels of access to the system depending on their requirements.
- All staff know that any information about children must always be encrypted and therefore any memory sticks, external hard drives, personal computers etc. must be encrypted. Encrypted memory sticks are provided by the school but it is the responsibility of the staff member to ensure that any personal equipment used is appropriately encrypted.

Internet and E-mail Access

Published content and the school web site

The school will publish its own address, e-mail and telephone number on the school website. Staff and pupils' personal information will never be published on the school's website.

The school's Headteacher will take overall editorial responsibility and ensure that content is both accurate and appropriate at all times.

Consent for publishing pupils' images and work

Written permission from parents or carers will be obtained annually before photographs of pupils will be published on the school website.

Once a consent form has been signed and returned, parents still retain the right to withdraw consent at any stage, but they need to do so in writing.

Pupils' full names will not be used anywhere on the website or on any published recording, podcast or video. In addition, any photographed children will not be named.

Safe surfing of the Internet

At Calow C of E Primary School we aim to keep our children safe when using the Internet. The school's ISP has a filtering system in place so that children are protected whilst using the Internet.

If pupils discover an unsuitable site, they will report it immediately to the member of staff who is present. The member of staff will make a note of the site, close the site and report it to the Online Safety Lead. The Online Safety Lead will inform the Headteacher and contact the ISP to ensure that they are informed and that the filtering system is being correctly applied. If necessary, the technician will be informed in order to verify filtering levels are appropriate.

Checks will be made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Social networking sites

The school's Internet Service provider blocks all social networking sites, so children are unable to access them at school. Facebook is accessible to staff, for access to the school's Facebook account only.

In addition, children are taught never to give out personal details of any kind which may identify them or their location.

Staff also have a responsibility to ensure that contact is not made between themselves and any pupils or parents (past or present) on social networking sites. They should also be aware that their sites could be viewed by parents or pupils if correct settings are not applied. Staff should remain professional in their conduct at all times and are discouraged from using social networking sites. No reference should be made in social media to pupils, parents / carers or staff. There should be no online discussion on personal matters relating to members of the school community and no personal opinions should be given about the school or local authority.

Staff should also ensure that their security settings on personal social media profiles are appropriate and regularly checked to minimise the risk of loss of personal information.

Further details are found in the Acceptable Use Policy.

E-mail

The official school email services may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

Pupils may only use approved class e-mail accounts on the school system.

Pupils (or staff) must immediately tell a member of staff if they receive 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.

Staff should not use private e-mails to contact any pupils or parents and should not give out such details to pupils or parents.

Mobile Devices

Pupils are strongly discouraged from bringing mobile phones or tablets into school. If they do bring them, they must be switched off at all times on school property (including outside, before and after school) and handed into the school office immediately until the end of the day. The school can accept no liability for loss or damage of these devices.

Staff should not give personal contact details such as mobile phone numbers to pupils or parents and should report any contact trying to be made through this method to the Headteacher.

Use of digital and video cameras and 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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students 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.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, storing and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should never be used for such purposes. These images are then downloaded onto the school's NAS drive to provide further protection from them being viewed or used by anyone else.

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. The school will not publish images of children on the school Facebook Page, unless with the express permission of parents/carers.

Pupils' full names will not be used anywhere on a website.

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

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

Appropriate Use

The school's digital technology resources are to be used to enhance learning and teaching and are not for private and/or personal use, unless the school's Headteacher has given specific permission. All staff are required to adhere to the Acceptable Use Policy.

Virus Protection

The school uses software to ensure that all networked machines are kept up to date against viruses.

Legal issues

- All of the school's software is legally licensed and catalogued.
- No software should be added to machines unless permission has been given by the school's Online Safety Lead.
- Staff must ensure that when using ICT material they are not infringing copyright laws.
- Staff should ensure that they are familiar with issues surrounding Creative Commons licensing.
- Subject Leaders must inform the School Business Officer when any new software purchased through their subject budget is received so that the software inventory can be updated.

Responding to incidents of misuse

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

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- grooming, incitement, arrangement or facilitation of sexual acts against children
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- terrorism or radicalisation
- other criminal conduct, activity or materials

the Headteacher will be informed and will inform the relevant authorities including Derbyshire LA and the police. All members of staff are under an obligation to be vigilant in these matters and immediately report any known or suspected illegal activity. (Please see the 'Illegal Incidents' flowchart in the appendices.)

Staff must ensure that if images of children are thought to be on a device or computer, they **must not** view them. If on a mobile phone, it should be turned to 'airplane mode' and placed in a secure place while the procedure outlined on the flowchart is followed. If on a computer,

then the computer should be isolated (any change to its state may hinder a later police investigation). There should be more than one member of staff present at each step of the procedure for protection against any subsequent accusations.

Search and delete

The Headteacher (or delegated member of staff) has the right to search for such electronic devices where they reasonably suspect that data or a file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - authorised staff may search with the pupil's consent for any item
- Searching without consent - authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item (as described above).
The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.
The authorised member of staff carrying out the search must be the same gender as the pupil being searched (where practically possible); and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.
A record should be kept of the reasons for the deletion of data / files.

Sexting and peer on peer abuse

Staff must be aware of the definition of 'sexting' and the legal implications for pupils and for themselves if they are involved in investigating a situation where sexting may be involved. Guidance should be followed from 'Sexting in Schools and Colleges: Responding to incidents and safeguarding young people. In particular, the information in section 2 - Handling Incidents - will be followed so that, where possible, the incident is dealt with in school (in partnership with home) to avoid the criminalisation of a child / children.
In dealing with incidents involving 'Sexting', the Headteacher, Designated Safeguarding Lead and Online Safety Lead will follow advice and act in the best interests of the child / children involved.
Staff must be aware that images and inappropriate messages may be sent between young people with the intention of causing harm or upset. Children are taught about 'Cyberbullying' through learning in PSHE, Computing and other lessons and issues that arise should be dealt with in accordance with the school's Anti-bullying Policy.

Other incidents

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that the Online Safety Lead Leader and Headteacher are immediately informed and correct procedures in line with School Policies and Derbyshire LA guidance will be used to investigate, preserve evidence and protect those carrying out the investigation.

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 in accordance with the school's Behaviour Policy.

Security of Digital Technology Resources

Calow Church of England (VC) Primary School has clear security measures to help protect its digital technology equipment.

- All equipment worth over £100 is recorded on the inventory.
- The Computing Suite is central within the school building and as such has no windows. This equipment cannot be viewed from outside the school
- Equipment is moved to the Computing Suite, which is a secure room, at the end of the day or portable items are placed in locked cupboards / filing cabinets.
- Class computers, where ever possible, will be kept out of sight or blinds / curtains will be closed. Security fencing around the school prevents any equipment being viewed from outside the school grounds.
- Mobile devices are not removed from school property unless being taken on an educational visit or with specific authorisation from the Headteacher.

Data Protection

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

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

The school must ensure that:
• 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.
• Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
• All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
• It has a Data Protection Policy
• It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
• It has clear and understood arrangements for the security, storage and transfer of personal data

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.
• 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 (staff are responsible for this)
• the device must be password protected (staff are responsible for this)

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

All members of the school community can save appropriate material onto the school network. The network is password protected to ensure that children cannot access any staff materials that are not for general curriculum use.

Informal checks ensure that only appropriate material is stored on the school's server.

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.

Privacy

The school will collect personal information about you fairly and will let you know how the school and Derbyshire LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Derbyshire LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Derbyshire LA.
The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Derbyshire County Council and as defined by the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Disposal of ICT Equipment

Calow Church of England (VC) Primary School will dispose of any ICT resources in line with current DCC protocol.

Governor approval will be sought before ICT resources are disposed. Following Governor approval, all equipment which contains sensitive files will have their hard disk drives destroyed, and serial numbers will be collected. Finally, the school's inventory will be updated.

This policy is consistent with Article 9 of the UN Convention on the Rights of the Child.

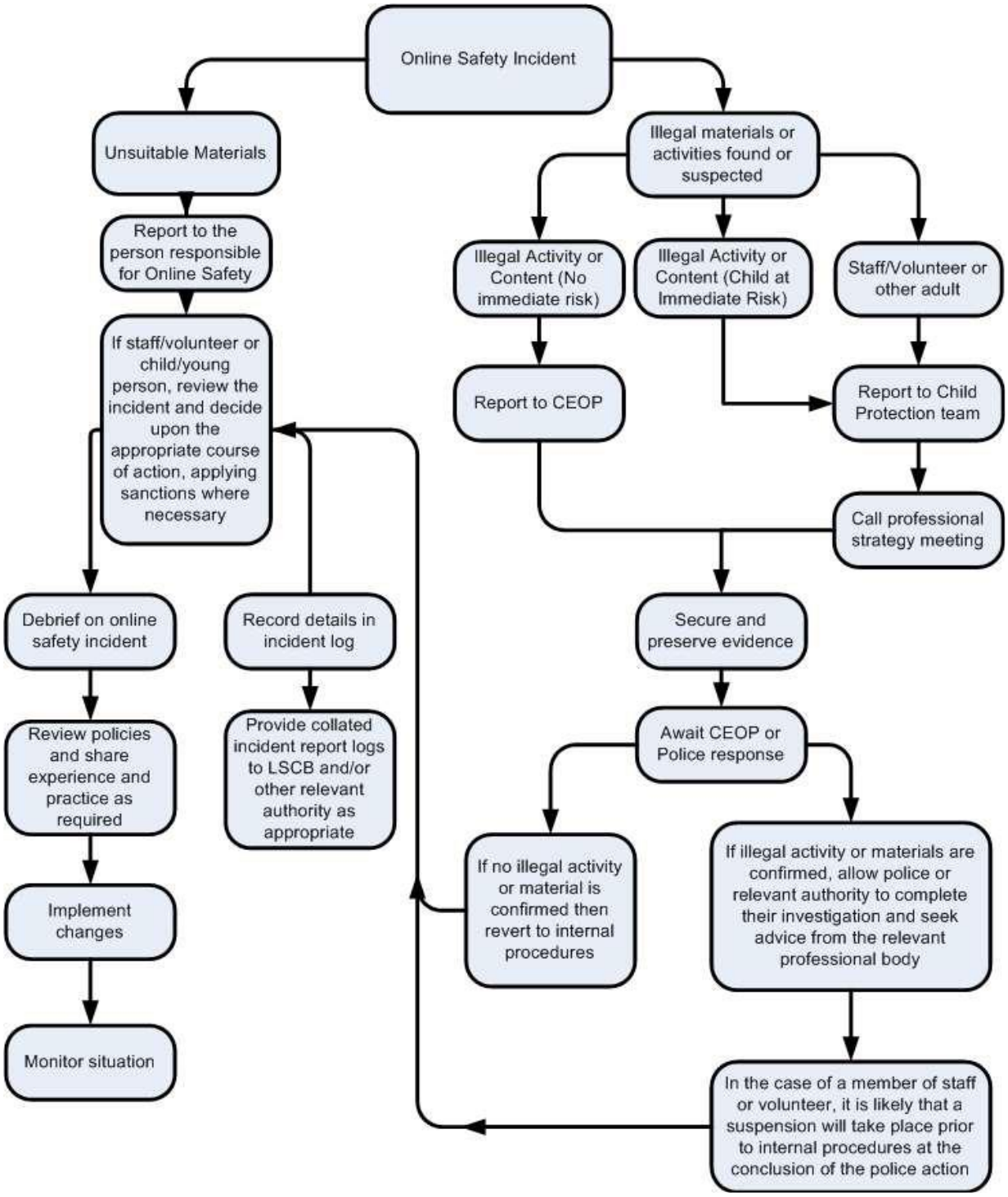
This policy should be read in conjunction with the Acceptable Use Policy, Computing Policy and all appropriate Safeguarding Policies. It is also consistent with The Prevent Duty issued by the DfE and Keeping Children Safe in Education 2016.

Policy written: November 2016
Policy approved by Governors:

Signed _____

Policy review: November 2017

Appendix


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

http://www.ictnews.az

Our Responsibilities

We are responsible for using Computing equipment correctly and safely, including computers, i-pads and cameras, and will speak to a member of staff if equipment is being misused. When we research, we will be able to tell you where we found the information. We will remember the online safety messages and rules that we have learned in school even when we are at home. These messages can be seen in all rooms where there is technology. We know that everything that we do online leaves a digital footprint which will stay with us throughout our online life. We know that we must keep our passwords safe.

http://internet-browser-review.toptenreviews.com/

Safe surfing of the Internet

There is a filtering system and firewall that keeps us safe when we use the internet in school. Adults check that the filters are working properly so that we can only look at safe information. We only use the internet when an adult is present. We know that we don't search on any images as they are not filtered. When we are finding information we know to check it as not all information is correct. We will turn our screen off or minimise it and tell an adult straight away if we find an unsuitable site. Our teacher will report the site to Mrs Oldale.

http://vedlo.com

Social Networking Sites

We are unable to go on social networking sites in school. We are taught never to share our name, address or other personal information when we are online. We know that we should have parental permission to use social networking; only talk to people that we know in real life and that we should not arrange to meet up with strangers. We know that it is important to check our privacy settings.

http://www.bbc.co.uk

Electronic Communication

We may only use our learning platform or ecadets 'bubble' to join in with discussions or to message adults in school. If we read an inappropriate message, we should not delete it but we should tell a trusted adult and show them the message. We know that we should only send polite messages and we only send or accept emails from people that we are friends with in real life.

https://www.mobilepro.co.uk

Mobile Phones

We are unable to bring mobile phones into school. If they are brought in for an emergency then they will be kept in the school office. Mobile phone numbers should not be shared without our parents' or carers' permission. We know that we should only play games on them or use apps that we have permission to from a trusted adult. We know that we must check with a parent before getting new contacts and that all messages sent should be polite.

http://www.which.co.uk

Use of digital cameras and images

We know that once a photograph is uploaded to the internet it is there forever as part of our digital footprint. We will use cameras and i-pads appropriately as part of our learning. We do not take or send photographs of other people without their permission.