Cowbit St Mary's Church of England School

E-Safety & Acceptable Use Policy (Staff)

Policy Statement

For clarity, the policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents, volunteers and visitors.

Safeguarding is a serious matter; at Cowbit St Mary's Church of England School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an incident, whichever is sooner.

The primary purpose of this policy is:

- To ensure the requirement to empower the whole school 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 foreseeability of harm to the pupils and staff or liability to the school.

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance at the school who will: Keep up to date with emerging risks and threats through technology use.

- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher
Reporting to the governing body, the Headteacher has overall responsibility for within our school. The day-to-day management of this will be delegated to a member of staff, the Officer.

The Headteacher will ensure that:

- training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.

- The designated Officer(s) has had appropriate CPD in order to undertake the day to day duties.

- All incidents are dealt with promptly and appropriately.

Officer
The day-to-day duty of Officer is devolved to the Headteacher.

The Officer will:
- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Headteacher.

- Advise the Headteacher, governing body on all matters.

- Engage with parents and the school community on matters at school and/or at home.

- Liaise with the local authority, IT technical support and other agencies as required.

- Retain responsibility for the incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

- Make him/herself aware of any reporting function with technical measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.

- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.

- Any technical solutions such as Internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the officer and Headteacher.

- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.

- Any incident is reported to the Officer (and an Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the Officer or the Headteacher to make a decision.

- The reporting flowcharts contained within this policy are fully understood.

- They are familiar with the guidance in the Professional Responsibilities regarding the private use of Social Networking sites compiled by Hertfordshire County Council and approved by a variety of Unions. (All members of staff have received a copy of this.)

Technology

Cowbit St Mary's Church of England School uses a range of devices including PC's, laptops, iPads, MacMini In order to safeguard the pupils and staff and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – This is to prevent unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – This helps to prevent any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and pupils should keep their unique username private.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as pen drives etc. are to be scanned for viruses before use.

Mobile Phones - The school allows staff to bring in personal mobile phones and devices for their own use outside lesson time. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Personal mobile phones should not be used for the taking of photographs of pupils, themselves or colleagues whilst at school. Photographs should always be taken using school equipment and should only be used for professional purposes.

Staff should **never** take photographs of themselves or other colleagues using mobile phones or similar devices at school and then post them on social networking sites.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this and the staff Acceptable Use Policy; pupils/parents upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Pupils are permitted to use the school email system under adult supervision, and as such will be given their own email address.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – is allowed in our school via restricted approved sites. Staff and children have received sufficient education in the dangers of Social Networking sites and have received appropriate guidance in their use.

Staff who use Social Networking sites in their private lives should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available.

All members of staff should never knowingly become 'friends' with pupils on any social networking site or engage with pupils on internet chat.

Likewise they should never knowingly become 'friends' with former pupils until they are sure that the former pupil is mature enough to accept the responsibility of the 'friendship', i.e. over the age of 18 years.

Staff should also think carefully about who they become 'friends' with particularly if those 'friends' are existing parents of children at the school. A parent who has shared private information as a 'friend' on a social networking site may well use that information at a later date should an issue arise that affects them or their child.

Skype is available on all Teacher laptops and is for use in school only. Personal use of the School Skype Account is NOT permissible.

Staff are not permitted to access their personal social media accounts using school equipment at any time. Likewise staff are not permitted to access their personal social media accounts during the school working day.

Your professional role should not be compromised in any capacity when using social media of any kind.

Members of staff should ensure that any online activity **both in school and outside school** will not bring Cowbit St Mary's Church of England School or your professional role into disrepute.

All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any incident is to be brought to the immediate attention of the Officer, or in his/her absence the Headteacher. The Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Cowbit St Mary's Church of England School will have an annual programme of training which is suitable to the audience. This will be carried out with the support of Lincolnshire Safeguarding Children Board.

for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupils' learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Why do we Filter and Monitor?

Schools filter Internet activity for two reasons:
We filter to ensure

- As much as possible that children and young people and to some extent adults are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.

- As much as possible that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- As much as possible that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' rules. However, some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of. Internet activities are planned and well managed for these children and young people.

Policy for Dealing with Radicalisation and Extremism

Cowbit St Mary's Church of England School adopts a robust approach to these issues, and remains alert for any signs of Radicalisation or Extremism.

Cowbit St Mary's Church of England School operates a Policy for dealing with Radicalisation and Extremism, and aims to provide an inclusive, caring and stimulating environment which enables all children to enjoy learning and reach their full potential. We welcome all families, irrespective of their faith or if they have no faith. We will ensure that all children feel safe, and are treated with respect, whilst promoting the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs. For further details, refer to the relevant school Policy.

A right to privacy?

Everybody at Cowbit St Mary's Church of England School has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

This Policy should be read in conjunction with the Anti-Bullying Policy, and Safeguarding/Child Protection Policy, Radicalisation and Extremism Policy.

This policy is available for anybody to read on the Cowbit St Mary's Church of England School website; upon review all members of staff will sign as read and understood both the policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Review

This Policy will be reviewed at least every two years.

Reviewed February 2018

Signed …….

Chair of Governors

___/___/___

Cowbit St Mary's Church of England School

Incident Log Number	Reported By (name of staff member)	Reported to (e.g. Headteacher, Officer)
When	When	When
Incident Description (Describe what happened, involving which children and/or staff, and what action was taken		
Review Date		
Result of Review		
Signature (Headteacher)	Date	
Signature (Governor)	Date	

Cowbit St Mary's Church of England School

Risk Log
(with examples)

Number	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet Browsing	Access to inappropriate/illegal content – staff	1	3	3	e-safety officer, IT support
2	Blogging	Inappropriate comments	2	1	2	
3	Internet Browsing	Access to inappropriate/illegal content – staff	2	3	6	
4	blogging	Using copyright material	2	2	4	

Likelihood How likely is it that the risk could happen (foreseeability)

Impact What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

SCORE 1-3 = Low Risk 4-6 = Medium Risk 7-9 = High Risk

Owner The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.

Final decision rests with Headteacher and Governing Body.