Online Safety Policy- Charter Primary School

This Online Safety policy has been developed by a working group including Headteacher, Senior Leaders, Online Safety Coordinator, Staff and Governors.

Approved:

Review date:

The school will monitor the impact of the policy using: logs of reported incidents, internal monitoring/filtering reports and surveys of pupils, parents and carers.

Scope of the Policy

This policy applies to all members of the *school* community who have access to and are users of school ICT 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 cyber-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. Action can only be taken over issues covered by the published 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

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
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors meeting

Headteacher and Senior Leaders:

- 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 Co-ordinator.*
- 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 appendix 1).
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator 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 / Senior Leaders 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.

<u>Online Safety Coordinator:</u>

- leads the Online Safety Group
- 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 school technical staff
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering/monitoring reports
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

<u>Network Manager / Technical staff:</u>

The Network Manager / Technical Staff is responsible for ensuring:

- 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 Online Safety Policy / 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher Online Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated

<u>Teaching and Support Staff</u>

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school* Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with students / 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
- 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

<u>Designated Safeguarding Lead</u>

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
- cyber-bullying

<u>Online Safety Group</u>

The Online Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. See appendix 2 for Online Safety Group Terms of Reference.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

<u>Pupils</u>
- 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
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good 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

<u>Parents / Carers</u>

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 *newsletters, letters, website and information about national / local online safety campaigns / 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 and the school blog
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

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 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 / PSHEE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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 on-line 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
- Letters, newsletters, web site, blog
- 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 (see appendix for further links / resources)

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

<u>Education & Training – Staff</u>

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 Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / 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 Coordinator will provide advice / guidance / training to individuals as required.

<u>Training – Governors</u>

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 / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school / academy 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 / academy 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
- Staff users are responsible for the security of their username and password and will be required to change their password every term.
- The "master / administrator" passwords for the school ICT system, 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 (eg school safe)
- OAKFORD 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 (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.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering.
- 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.

Responding to incidents of misuse

Staff will follow the guidance flowchart in appendix one when responding to incidents of misuse. 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 (appendix 1) for responding to online safety incidents and report immediately to the police.

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 / volunteer 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 / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action

- **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:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - 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.

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 outlined in the code of conduct.

Acceptable user agreement-

All members of school including volunteers will sign acceptable user agreements which includes information regarding mobile technology, social media and communications.

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 students / 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.
- Written permission from parents or carers will be obtained before photographs of students / 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 / academy 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 social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy 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.
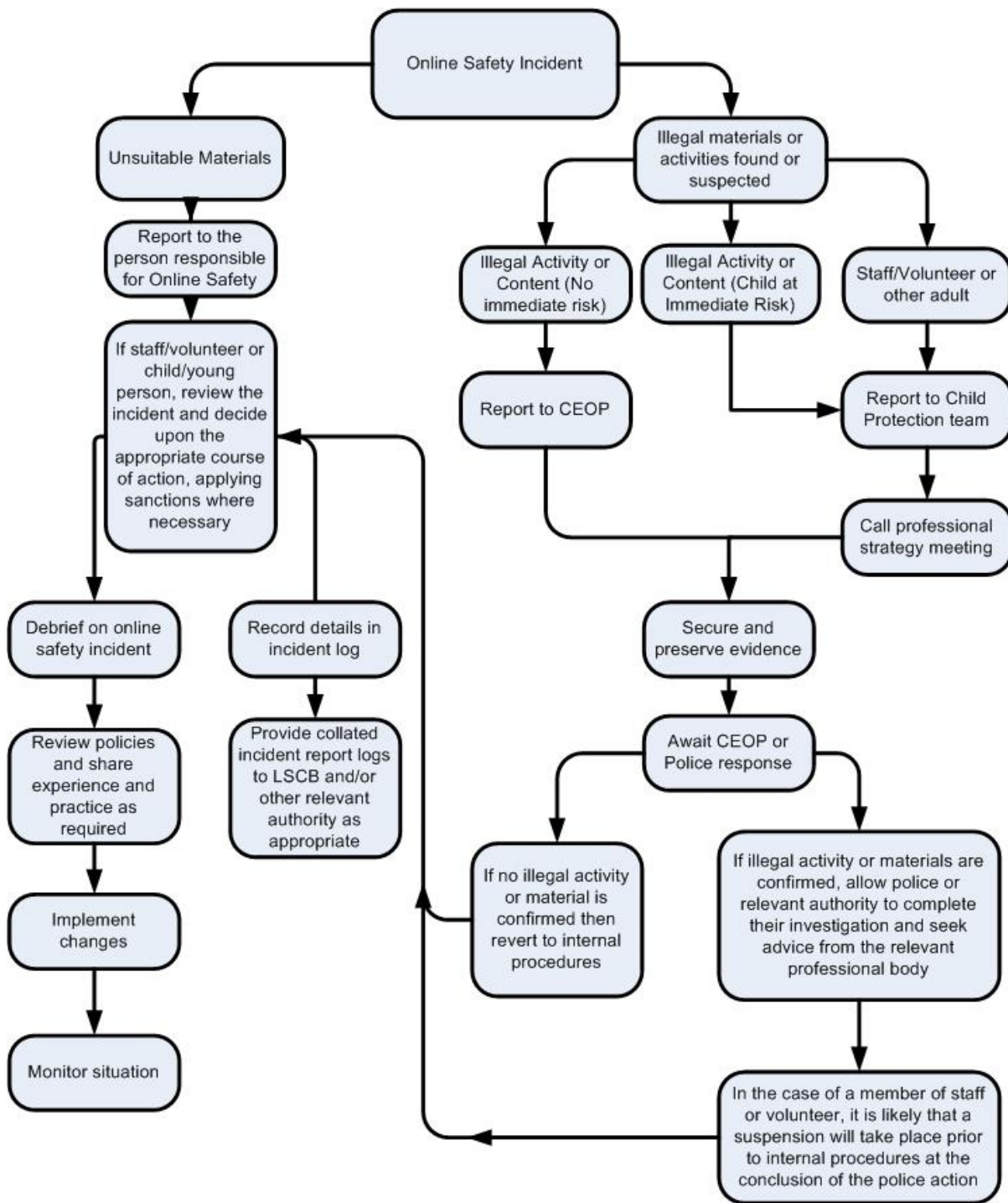
Use of mobile technologies

- During class time, all personal mobile phones should be placed in a locked cupboard, on silent.
- Personal phones should not be used to make or receive any communication during class time.
- Break times, lunchtimes or after school hours should be used for dealing with any incoming and outgoing communication.
- Between the hours of 8.00am and 4.30pm, any personal telephone conversations or communication should take place in a classroom where no children are present.
- Personal mobile phones should all be security pin coded as a minimum requirement.
- During reading sessions, playtimes and lunchtimes, e- readers can be used by both staff and children. 4G is not to be used.
- Children bringing personal mobile phones to school must place them in the appropriate cupboard and turn them off. Any child with permission from adults to walk home may have a personal mobile phone in school.
- On school trips, the school mobile (which is pin locked) must be taken to make calls. The school iPad (which is pin locked) must be used to take photographs. Personal mobile phones should not be used where children are present. Parent helpers should not use their mobile phones on trips.

Appendix 1.

Responding to incidents of misuse – flow chart

Online Safety Incident

Branch 1 — Unsuitable Materials

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

Branch 2 — Illegal materials or activities found or suspected

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

Appendix 2

<u>Online Safety Group Terms of Reference</u>

1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1.   The   online   safety   group   will   seek   to   include   representation   from   all   stakeholders.

        The composition of the group should include :
- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator
- Governor
- Parent / Carer
- Student digital leaders – for advice and feedback. Pupil voice is essential in the make-up of the online safety group, but pupils would only be expected to take part in committee meetings where deemed relevant.

2.2.   Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3.   Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4.   Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5.   When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held every term for a period of one hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Co-ordinator with the following

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety.

- Staff meetings
- Student / pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Website/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Charter have been agreed

Signed by (SLT): --

Date: --

Date for review: --

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council