Designated Safeguarding Lead Mr G Sayers

Date written: September 2018

Reviewed: July 2019

Date of next review July 2020.

This protocol will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Online safety is an essential part of safeguarding, the internet and technology-based devices are an essential part of everyday life and pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

- The purpose of this protocol is to:
    - Safeguard and protect all members of the school, online.
    - Identify approaches to educate and raise awareness of online safety.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- Issues classified within online safety may be considerable, but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

- This protocol links with:
    - Anti-bullying protocols.
    - Acceptable Use protocols for staff and statement for pupils.
    - Child protection policy.
    - Values education.
    - Tutor time activities.
    - Procedures for reporting welfare concerns to a designated safeguarding lead.

Leadership and Management

Online safety is viewed as a safeguarding issue, acceptable use agreements are included in staff safeguarding training and the process for reporting concerns is the same as any other safeguarding issue. There is open dialogue between the IT manager and the lead safeguarding officer to ensure that online safety has the prominence it requires. The acceptable use agreement is comprehensive and should be read alongside this protocol. The agreement includes social media use, email expectations, use of personal devices and communication.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other m embers of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this within the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.

- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the management team and to the safeguarding governor through regular meetings.

It is the responsibility of all members of staff to:

- Read and adhere to the online safety protocol and acceptable use protocols.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Staff personal mobile phones should not be used whilst involved in professional duties such as teaching or on duty.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

- To support pupils to read and understand the pupil acceptable use statement in a way which suits their age and ability.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.

- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

It is the responsibility of pupils to:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the school acceptable use statement.

Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in relevant programmes of study.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Training and engagement with staff

The school will:

- Provide and discuss online safety with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Classroom Use

- We use a wide range of technology that includes:
    - Computers, laptops, tablets and iPads
    - Internet which may include search engines and educational websites
    - School learning platform/intranet
    - Email
    - Digital cameras, web cams and video cameras

- All school owned devices will be used in accordance with the school's acceptable use agreement and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully and discuss their use with the DSL before use in the classroom or recommending for use at home.
- Staff must log the device number and pupil details when issuing devices to students before use.

Filtering

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

- The school uses educational broadband connectivity through Kent Public Service Network (KPSN)
- The school uses light speed and EIS which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school works with KPSN and EIS to ensure that our filtering policy is continually reviewed.
- Other sites may also be filtered out following a risk assessment by the DSL and the IT manager.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they are encouraged to tell a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - Parents/carers will be informed of filtering breaches involving their child that are a safeguarding concern.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

Monitoring

The technical team get a weekly report from lightspeed and EIS which identifies the user, website and time of the search. Any questionable usage will be reported to the DSL.

Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.

- Regularly checking files held on the school's network,
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Passwords

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private. Passwords should have at least 8 characters including capital letters, numbers and punctuation.
- Pupils are provided with their own unique username and their passwords should have at least 6 characters including capital letters, numbers and punctuation.

Safeguarding

- Responding to online safety incidents and concerns, sexting and radicalization are dealt with through the safeguarding policy and acceptable use agreements. Cyber bullying is dealt with through our anti bullying protocols. Specific education is provided to help young people deal with issues such as exploitation and the sharing of images which can occur using the internet.