St John's Mead School

Valuing Effort, Valuing Others, Valuing Self

On Line Safety Policy

Policy Number	**17**
Version	**04**
Policy Date	**September 2016**
Review Date	**September 2018**

St JOHNS MEAD
On Line Safety Policy

TABLE OF CONTENTS

1 DEVELOPMENT MONITORING AND REVIEW

This Online Safety policy has been developed by a committee made up of:
- Headteacher
- Online Safety Coordinator
- Staff – including Teachers & Support Staff
- Governors
- Parents and Carers

Consultation with the whole school has taken place through a range of formal and informal meetings.

2 SCHEDULE FOR DEVELOPMENT, MONITOING AND REVIEW

This policy was approved by the Board of Governors on:	(DATE)
The implementation of this Online Safety policy will be monitored by the:	Online Safety Coordinator
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2017
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, Police

3 SCOPE OF POLICY

This policy applies to all members of the school including staff, pupils, volunteers, parents & carers and visitors 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. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, 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.

4 ROLES AND RESPONSIBILITES

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

4.1 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:

- attendance at Online Safety meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs

4.2 Headteacher and School Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.

- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management 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.
- The Headteacher is 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 will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

4.3 Online Safety Coordinator

- 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 the Local Authority and other relevant bodies.
- liaises with school technical staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety Governor to discuss current issues and review incident logs
- attends relevant meetings.
- reports regularly to Senior Leadership Team.

4.4 Network Management

The school's technical support is provided by an outside ICT service.

The network manager 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 any Local Authority Online Safety Policy or 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
- that filtering 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, Learning Platform, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation
- that monitoring systems are implemented and updated as agreed in policies

4.5 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher for investigation
- all digital communications with students, 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
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students 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

4.6 Designated Safeguarding Lead

The Designated Safeguarding Lead should be trained in Online Safety issues and be aware of the potential for serious child protections issues to arise from:

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

4.7 IT Coordinator

The IT Coordinator will be responsible for:

- the production, review & monitoring of the school Online Safety Policy
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression, through use of the South Gloucestershire Scheme of Work.
- consulting stakeholders – including parents & carers and the student about the online safety provision
- monitoring improvement actions

4.8 Students

Students will:

- be responsible for using the school digital technology systems in accordance with the Student 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 and use of images and on cyber-bullying.
- 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

4.9 Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and the school website and information about national & local online safety campaigns and 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
- their children's personal devices in the school (if this is ever relevant)

5 Policy Statements

5.1 Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of the Computing curriculum and is regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of assemblies
- Students will be taught in all relevant lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will 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.
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, students will be guided to sites checked as suitable for their use and informed of processes for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.

5.2 Education - Parents and 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 and 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:

- Letters, newsletters, web site, Learning Platform
- Parents & Carers evenings
- 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

5.3 Education & Training – Staff

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 programme of online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The IT Coordinator will receive regular updates through attendance at external training events 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 meetings.
- The IT Coordinator / Officer will provide advice, guidance and training to individuals as required.

5.4 Education & Training – Governors

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

- Attendance at training provided by the Local Authority or other relevant organisation
- Participation in school training or information sessions for staff or parents, which may include attendance at assemblies and lessons

6 TECHNICAL – INFRASTRUCTURE, EQUIPMENT, FILTERING AND MONITORING

The school has a managed IT service provided by an outside contractor, however It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the school Online Safety Policy and Acceptable Use Agreements. The school will check their Local Authority or other relevant body policies on these technical issues. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also 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 as outlined in Local Authority policy and guidance
• There will be regular reviews and audits of the safety and security of school technical systems
• Servers, wireless systems and cabling will 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. Users are responsible for the security of their username and password and will be required to change their password regularly. In the foundation stage, children will be given a class login.
• The managed IT service 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 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 will ensure that children are safe from terrorist and extremist material when accessing the internet.
• 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 or potential technical incident or security breach to the Headteacher.
• 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.
• School Supply Teachers will be provided with a temporary login onto the school systems.

7 MOBILE TECHNOLOGIES AND COMMUNICATION

Personal Mobile Technologies, such as phones, tablets, notebooks and laptops will not have the capability of using the school network and infrastructure, however may be present in school.

•Student owned devices that are brought into school should be turned off and kept by teacher or other relevant person until end of school day at the risk of the student.
•Staff owned devices can be brought into school but should not be used for school business.
The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems
• Users must immediately report to the Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
• Any digital communication between staff and parents & carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
• Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

8 USE OF DIGITAL IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents & carers and students 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 students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website, social media, local press signed by parents or carers at the start of the year
- Parents & carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents & carers comment on any activities involving other students in the digital or video images
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission • Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.

9 SOCIAL MEDIA

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. School and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

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

School staff should ensure that:

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

Official school social media accounts will have:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including

- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

9.1 Personal Use

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

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

9.2 Monitoring of Social Media

The school will monitor the Internet for public postings about the school and respond accordingly. The school's use of social media for professional purposes will be checked regularly to ensure compliance with the school policies.

9.3 Unsuitable/Inappropriate Activities

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

- Child Sexual Abuse Images
- Grooming, incitement, arrangement or facilitation of sexual acts against children
- Possession of extreme pornographic images
- Criminally racist material
- Pornography
- Promotion of any form of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school.
- Using school systems to run a private business
- Using systems that bypass filtering or other safeguards
- Infringing copyright
- Creating or propagating computer viruses
- Unfair usage e.g. downloading large amounts that hinder others' usage.

10 RESPONSE TO MISUSE

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

• Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
• It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
• Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures o 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. The completed form should be retained by the group for evidence and reference purposes.

11 ACTIONS AND 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 disciplinary procedures.