Sandwell Community School

e-Safety Policy

Safeguarding pupils, staff and school in a digital world

2015/16

Contents

1. Introduction

2. Responsibilities of the School Community

3. Teaching and Learning

4. Parents and carers

5. Managing and safeguarding ICT Systems

6. Safe and responsible use - using the Internet; email; publishing content online; using images, video & sound; using video conferencing and other online text or video meetings; using mobile phones; using other technologies

7. Protecting school data and information

7a. The Prevent Duty

8. Dealing with e-Safety incidents

9. Acceptable Use Policies (AUP) (Staff, temporary or supply staff, Pupils)

9a. Example letter to Parents

10. Ratification

Acknowledgement

This document is based on an original document '**YHGfL Guidance for creating an e-Safety Policy'** produced by the YHGfL e-Safety Officer and Ofsted – Inspecting e-Safety in schools (April 2014). Both adapted and updated by Mazer Iqbal and Debbie Stewart for SCS in January 2016.

1. Introduction

This e-Safety policy recognises the commitment of our school to e-Safety and acknowledges its part in the school's overall Safeguarding policies and procedures including Ofsted's guidance. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to e-Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

The scope of this policy

This policy applies to the whole school community including the senior management team (SMT), governors, all staff employed directly or indirectly by the school, visitors and all pupils.

The senior management team and governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safety within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers head teachers, 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 e-Safety-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the head teacher believes it contains any material that could be used to bully or harass others.

The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-Safety behaviour that take place out of school.

Implementation of the policy

The senior management team will ensure all members of school staff are aware of the contents of the school e-Safety policy and the use of any new technology within school.

All staff, pupils, occasional and external users of our school ICT equipment will sign the relevant Acceptable Use Policies

All amendments will be published and awareness sessions will be held for all members of the school community.

e-Safety will be taught as part of the curriculum in an age-appropriate way to all pupils.

e-Safety posters will be prominently displayed around the school.

The e-Safety policy will be made available to parents, carers and others via the schools website www.sandwellcs.org.uk.

The following local and national guidance are acknowledged and included as part of our e-Safety policy:

SCSB Guidance

Sandwell Safeguarding Children's Board Procedures and Guidance

Sandwell Safeguarding procedures will be followed where an e-Safety issue occurs which gives rise to any concerns related to Child Protection. In particular we acknowledge the specific guidance in:

4.3.2 Child Abuse and Information Communication Technology

This section of the SCS Safeguarding procedures covers awareness of, and response to, issues related to child abuse and the Internet. In particular we note and will follow the advice given in the following section:

Official Guidance

Guidance for Safer Working Practices for Adults who work with Children and Young People produced by DCSF in Jan 2009 and still current

This guidance provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. We acknowledge the guidance given in the following sections and accept this as part of our policy. (See extract in Appendix)

- **Section 12 Communication with Children and Young People**

- **Section 27 Photography and Videos**

- **Section 28 Access to inappropriate images and Internet Usage**

- **Inspecting e-Safety in schools – Ofsted April 2014**
www.ofsted.gov.uk/resources/120196

This briefing aims to support inspectors in reviewing school's safeguarding arrangements when carrying out section 5 inspections.

The following SCS Guidance documents are included as part of this e-Safety policy:

Electronic Communications Guidance for Staff

e-Safety Incident Screening Tool

2. Responsibilities of the School Community

We believe that e-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The senior management team accepts the following responsibilities:

- The Executive Head will take ultimate responsibility for the e-Safety of the school community.
- Identify a person (the e-Safety lead) to take day to day responsibility for e-Safety; provide them with training; monitor and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system.
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets.
- Ensure liaison with the governors.
- Develop and promote an e-Safety culture within the school community.
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have e-Safety included as part of their induction procedures.
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to e-Safety.
- Receive and regularly review e-Safety incident logs; ensure that the correct procedures are followed should an e-Safety incident occur in school and review incidents to see if further action is required.
- Amend policy in line with any new Ofsted criteria or government legislation

e-Safety Lead

Responsibilities include:

- Taking day to day responsibility for e-safety issues and having a leading role in establishing and reviewing the school e-safety policies and supporting documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority.
- Liaising with the schools SIRO and AIO to ensure all school data and information is kept safe and secure.
- Liaising with school ICT technical staff and/or school contact from the managed service provider – Agilisys/Broadband Sandwell.
- Create and maintain a system for receiving reports of e-safety incidents and creating a log of incidents to aid future e-safety developments.
- Meeting with relevant staff to discuss current issues, review incident logs and filtering
- Attending relevant meetings.
- Reporting regularly to SMT.

All Staff

Responsibilities include ensuring that they:

- Read, understand and help promote the school's online safety policies and guidance.
- Read, understand and adhere to the staff AUP.
- Take responsibility for ensuring the safety of sensitive school data and information.
- Develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, **NEVER** through personal email, text, mobile phone social network or other online medium.

- Embed e-Safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.
- Report all e-Safety incidents which occur in the appropriate log and/or to their line manager. Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date.
- Ensure that provision exists for misuse detection and malicious attack.
- At the request of the leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed.
- Report any e-Safety-related issues that come to their attention to the e-Safety lead and/or senior leadership team.
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management.
- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment.
- Liaise with the Local Authority and others on e-Safety issues.
- Document all technical procedures and review them for accuracy at appropriate intervals.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Responsibilities of pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance.
- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening.

- Report all e-Safety incidents to appropriate members of staff.
- Engage all pupils and ensure that they complete all e-safety activities delivered via the school curriculum
- Discuss e-Safety issues with family and friends in an open and honest way.
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices.
- To know, understand and follow school policies regarding Cyber bullying.

Responsibilities of Parents and Carers

- Help and support the school in promoting e-Safety.
- Read, understand and promote the pupil AUP with their children.
- Discuss e-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Consult with the school if they have any concerns about their child's use of technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of pupils.

Responsibilities of the School Governors

- Read, understand, contribute to and help promote the school's e-Safety policies and guidance as part of the school's overarching Safeguarding procedures.
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safety awareness.
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data.
- Ensure appropriate funding and resources are available for the school to implement their e-Safety strategy

Responsibilities of the Child Protection Officer

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information. Data will be managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.
- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, cyber bullying etc.
- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to e-Safety ensuring that staff know the correct child protection procedures to follow.

Responsibility of any external users of the school systems

- Take responsibility for liaising with the school on appropriate use of the school's IT equipment and internet, including providing an appropriate level of supervision where required
- Ensure that participants sign and follow agreed Acceptable Use Procedures.

3. Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver an age appropriate e-safety curriculum that is flexible, relevant and engaging. It will promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. We believe that learning about e-Safety should be embedded across the curriculum and also taught in specific lessons such as in Computing/ICT and PSHE.

We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the AUP.

Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

4. How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and school website. The school newsletter will include the latest Government announcements about Internet Safety and a practical guide for parents and carers whose children are using social media.

We will ask all parents to discuss the pupil's AUP with their child and return a signed copy to the school.

We request our parents to support the school in applying the e-Safety policy.

5. Managing and safeguarding IT systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. head teacher and member of technical support.

The wireless network is protected by a secure log on which prevents unauthorised access. New users can only be given access by named individuals e.g. a member of technical support.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by BBS. This ensures that all reasonable precautions are taken to prevent access to illegal content. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

Any inappropriate websites which are not filtered will be recorded and passed onto BBS in order for them to be blocked.

Notices are posted in classrooms and around school as a reminder of how to seek help.

Access to school systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords. SCS Policies/AUP/RSJ Not Protectively Marked Page 13

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorizing and protecting login and password information.

Detailed guidance on the protection of sensitive school data and information assets is included in the **SCS Information Security Guidance** which forms part of this policy.

Passwords

We ensure that a secure username and password convention exists for all system access (email, network access, school management information system).

We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.

All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school.

All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

The school maintains a log of all accesses by users and of their activities while using the system in order to track any e-Safety incidents.

6. Safe and responsible use

Using the Internet

We provide the internet to

- Support curriculum development in all subjects.
- Support the professional work of staff as an essential professional tool.

- Enhance the school's management information and business administration systems.
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others.

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school ICT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently.

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and the school provides all members of the school community with an email account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. Email messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

Use of the school email system is monitored and can be checked.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils on the out-of-school times when emails may be answered.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

Publishing content online

E.g. using Website, Google drive/Moodle, blogs, wikis, podcasts, social network sites

School website/Google Drive:

The school maintains editorial responsibility for any publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the website is the school address, email and telephone number.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the website and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website/VLE.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

Using video conferencing, web cameras and other online meetings

Video conferencing can be used to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils will take part in these opportunities in a safe and responsible manner. All video conferencing activity will be supervised by a suitable member of staff. Pupils will not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the head teacher or line manager and respective parents and carers.

Using mobile phones

During lesson time we expect all mobile phones belonging to staff to be switched off unless there is a specific agreement for this not to be the case.

Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. (*In an emergency, where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.)*

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a website which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member we do not consider it a defence that the activity took place outside school hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyber bullying', will be considered a disciplinary matter.

We make it clear to staff, pupils and parents that the Head teacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

Mobile phones belonging to pupils are collected in on arrival to school.

Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for pupils. However their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

Pupils are taught to use them responsibly.

Using other technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an e-Safety point of view.

We will regularly review the e-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

7. Protecting school data and information

School recognises their obligation to safeguard staff and pupil's sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The school is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

Pupils are taught about the need to protect their own personal data as part of their e-Safety awareness and the risks resulting from giving this away to third parties.

Staff are made aware of the contents of the **SCS Information Security Policy for Staff**.

Management of assets

Details of all school-owned hardware and software are recorded in an inventory.

All redundant ICT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

7a. The Prevent Duty

The UK Government passed a new law on the 1 July 2015, the Counter-Terrorism and Security Act.

Known as the Prevent Duty this new legislation places a statutory requirement on all schools to ensure that they are taking proactive steps to identify any students who may be at risk of being drawn into extremism or influenced by the process of radicalisation.

Online radicalisation is one avenue that we are aware of and we make sure there are strategies in place to provide early intervention via Prevent where necessary.

8. Dealing with e-Safety incidents

All e-Safety incidents are recorded in the school e-Safety Log or on SIMS behaviour logs.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious e-Safety incident, concerning pupils or staff, they will inform the e-Safety Lead, their Line Manager or Head teacher who will then respond in the most appropriate manner. **[e-Safety Incident Guidance for Staff]**

Instances of **cyberbullying** will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's e-Safety Lead and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the SCS Safeguarding Procedures and Guidance will be followed.

4.3.2 Child Abuse and Information Communication Technology Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly.
- Responsibility for handling serious incidents will be given to a senior member of staff.
- Parents and the pupil will work in partnership with staff to resolve any issues arising.
- Restorative practice will be used to support the victims.
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

9. Acceptable Use Policies (AUP)

School has a number of AUPs for different groups of users.

These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate AUP.

Acceptable Use Policy for staff

I confirm that I have read and understood the **SCS Electronic Communications Guidance for Staff** and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document. In particular:

- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school.
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents.
- If I use instant messaging, chat rooms, webcams or forums for communicating with pupils or parents it will only be via the school's accredited system or website.
- Personal use of mobile phones/devices during my working day is not appropriate unless it is break/lunchtime and away from the pupils.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will take all reasonable steps to ensure that all laptops and memory devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

- I confirm I have read the **SCS Data Security Guidance for Staff** and will implement the guidelines indicated. In particular:

- Confidential school information, pupil information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended.
- I understand that I have the same obligation to protect school data when working on a computer outside school.
- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

I understand that the school may monitor or check my use of ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name……………………………………………………………………………………

Signed………………………………………………………………………

Date………………………………..

Acceptable Use Policy for temporary or supply staff and visitors to school

As a visitor to the school I recognise that it is my responsibility to follow school e-Safety procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned.
- I will not give my personal contact details such as email address, mobile phone number, IM account details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to VC or use a web camera with pupils unless specific permission is given.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date.
- I will only use my personal mobile phone during non-teaching time and away from students.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- If I have access to any confidential school information, pupil information or data, it will only be removed from the school site

with permission and if so, it will be carried on a device which is encrypted or protected with a strong password.

- I will report immediately any accidental loss of confidential information to a senior member of staff so that appropriate action can be taken.
- I understand that I have a duty of care to ensure that pupils in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school may monitor or check my use of ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the disciplinary procedures.

Name………………………………………………………………………………………

Signed……………………………………………………………………………

Date……………………

Acceptable Use Policy for pupils

I understand that use of the Internet and electronic communication is granted to me as a privilege, in return for my acceptance of this agreement. Any misuse on my part may result in loss of that privilege and other sanctions being taken. This also applies to any activity undertaken outside school which breaks the acceptable use rules of the school.

All online activity will be appropriate to:

- ensure the safety and security of the school system
- ensure respect for all members of the community
- maintain the reputation of the school

In particular this means:

- I will only access the school ICT system and Internet via my authorised account and password, which I will not make available to others.
- I will ensure that I do not wilfully damage the system by means of malicious code (e.g. virus infections, malware etc.), hacking or physical tampering.
- Language which I use in electronic communication will be appropriate and suitable, as for all school work.
- I will respect copyright of all materials.
- I will not wilfully interfere with and/or delete another person’s work files.
- I will not send or forward messages, publish or create material which is offensive, hurtful or otherwise upsetting to another person. Nor will I post anonymous messages or forward chain letters.
- I will not use a mobile phone, camera or other electronic device to take, publish or circulate pictures or videos of anyone without their permission.

In addition I understand that:

- Use of the network to knowingly access inappropriate materials such as pornographic, racist or offensive material is forbidden and may constitute a criminal offence.
- Guidelines for safe use of the Internet must be followed and I will report any materials or conduct which I feel is unacceptable.
- The school reserves the right to examine or delete any files that may be held on its computer system, to monitor any websites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

Full name…………………………………………………………………..

Signed………………………………………………….. Date…………..

Parent’s Signature ………………………………………………….. Date…………..

(Example Letter) Dear Parents

Safe use of the internet and email in school

As part of the national curriculum, pupils use computers in school to access the internet and to send email. Teaching pupils about safe use of these facilities is included as part of the curriculum. Your child will be introduced to e-Safety in a planned way through school to help them understand how to keep themselves safe when using the internet and other electronic devices. We will ensure that safe use is always included when new activities are introduced to pupils.

As part of our commitment to their safety we always ensure that access to the internet has a valuable educational purpose and is supervised. Internet access is provided through a filtered system which prevents access to the majority of undesirable material. However there is always a small chance that undesirable material can get through the filters but we will teach the children what to do should this occur. We will educate pupils to act responsibly on the internet and to understand some of the risks involved.

When pupils use any form of electronic communication, this will always be in a carefully controlled way so that we know who pupils are in contact with.

Many children now have access to the internet outside school, some via their mobile phones. You should be aware this offers pupils much more freedom to use the internet and consequently more ready access to material and activities which might be considered unsuitable. Pupils may also use this freedom to make contact with people they do not actually know, although they may consider them their friends, because they make contact with them on a regular basis. Pupils may also use some of these facilities (such as text messaging, cameras on mobile phones or social network sites such as Facebook) to send upsetting messages or publish things about other pupils which could count as bullying.

We will teach pupils about ‘cyber bullying’ and the danger of making contact with strangers online as part of the curriculum. We want you to know that we take any activity of this kind seriously even if it takes place outside school, as it can be seriously upsetting for the recipient.

We would contact you if an issue of this kind were to arise and would ask for your support in dealing with issues.

I enclose a copy of the Acceptable Use Policy that we operate at our school, which your child is expected to follow.

Yours sincerely

10. Ratification

D Smith

Acting Executive Head

Date: 01.03.16

Signed:…………………………………………………….

J McBride

Chair of Governors

Date: 01.03.16

Signed:…………………………………………………….

Implementation: 01.03.2016 (Academic Year 2015-16)

Review Date: February 2017