Shakespeare Primary School

Online Safety Policy

Date on which policy was approved: December 2016
Policy review date: 2019/20
Contents

Rationale
Aims
Development of this policy
Scope of the policy
Roles and Responsibilities
  Governors
  Headteacher and Senior Leaders
  Online Safety Coordinator
  Network Manager
  Teaching and Support Staff
  Designated person for child protection
  Online Safety Group
  Pupils
  Parents/Carers
Policy Statements
  Education—Pupils
  Education—Parents/Carers
  Education—The Wider Community
  Education & Training—Staff/Volunteers
  Education—Governors
  Curriculum
  Technical—infrastructure, filtering and monitoring
  Use of Digital and Video Images
  Data Protection
  Safeguarding
  Communications
  Social Media
  Unsuitable & Inappropriate Activities
  Illegal Incidents
  Other Incidents
  Responding to Incidents of Misuse
Appendix 1—Access Rights for School Computer System
Appendix 2—Responding to Incidents of misuse—flowchart
Appendix 3—Online Safety Incident Report Sheet
Appendix 4—Procedure for Temporary Guests
Appendix 5—Procedure for Misuse by Pupils
Appendix 6—Procedure for Misuse by Staff
Rationale
Computing and new technologies are an integral part of the lives of children and young people in today’s society. Shakespeare Primary School aims to actively enhance pupil’s experiences of this, both within school and in their lives outside school. We recognise that the internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.
We know that children and young people have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all staff at Shakespeare Primary School are bound. This online safety policy will help to ensure safe and appropriate use.

Aims
The aim of the Online Safety Policy is to promote safe, appropriate and consistent practice for all users whilst using the internet. The Policy records that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce risks. The Policy also addresses wider educational issues in order to help young people (and their parents/carers) to be responsible safe users.
Whilst we attempt to minimise risk we also recognise that it is impossible to eliminate all risk completely. This policy, therefore, identifies educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

It is important that this policy is used in conjunction with other school policies including the data protection policy, mobile phone policy and school Child Protection and Safeguarding policy.

Development of this Policy
This policy is based upon the Online Safety policy provided by SWGFL and adapted to meet the needs of the school.
The policy was discussed with staff on Tuesday 13th December and agreed by staff.
The policy is due for renewal in 2020 or earlier if required.

Scope of the Policy
This policy applies to all members of the school community including staff, pupils, volunteers, parents/carers and visitors who have access to and are users of school ICT systems, both in and out of school.
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 online safety incidents covered by this policy, which may take place out of 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. 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 roles and responsibilities for online safety of individuals and groups within the school.

Governors:
Governors will be responsible for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about e-safety incidents and monitoring reports.
The role of the Online Safety Governor will include:
• Annually, or as needed, meetings with the Online Safety Co-ordinator.
• Annual monitoring of online safety incident logs.
• Reporting to other relevant Governors.

Head Teacher and Senior Leaders:
• The Head teacher 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 Mrs T Skingle the Online Safety Co-ordinator.
• The Head teacher and Senior Leaders should be aware of the procedures to be followed in the event of a serious online safety allegation made against a member of staff (see flow chart on dealing with online safety incidents).
• The Head teacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
• The Head teacher and 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.
• The Online Safety Team and the Communication, Language and E-Learning team will receive regular monitoring reports (3x year) from the Online Safety Co-ordinator.
• The Head teacher (and Online Safety Coordinator) will receive emails from ‘Whisper’ and respond with appropriate measures, including forwarding concerns to the appropriate member of staff for further action.
• The Head teacher and 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.

Online Safety Coordinator
• Leads the Online Safety Group
• Reports regularly at Curriculum Team meetings.
• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy.
• Will receive emails from ‘Whisper’ and respond with appropriate measures, including forwarding concerns to the appropriate member of staff for further action.
• Ensures that all staff are aware of the procedures that need to be followed in the event of online safety incident taking place.
• Provides training and advice for staff.
• Liaises with school ICT technician – Mr M Norton.
• Receives reports of online safety incidents and creates a log of incidents to inform future developments. (Kept in office)
• Meets yearly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
• Attends relevant meetings with of Governors.
• Reports 3 times per year to Head Teacher

Network Manager
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 the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
• That users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularly changed.
• SWGfL is informed of issues relating to the filtering applied by the Grid.
• That he keeps 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 Online Safety Co-ordinator for investigation.
• To ensure the BOOST ‘Whisper’ is maintained and working on the school website.

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 school Staff Acceptable Use Agreement (annually).
• They report any suspected misuse or problem to their Phase Team Leader and Online Safety Coordinator for investigation.
• All digital communications with pupils and parents 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 school activities.
• Pupils understand and follow the school online safety and acceptable use policy.
• The monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices.
• In lessons where internet use is pre-planned pupils 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.
• Pupils know how to report a ‘Whisper’ incident from the school website.
• They respond quickly to any ‘Whisper’ reports sent to them and resolve issues in the correct manner promptly.

Designated Safeguarding Lead
Should be trained in online safety issues and be aware of the potential for serious child protection 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.

Online Safety Group
The Online Safety Group provides a consultative group that has responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. This group is also responsible for regular reporting to the Governing Body.
Members of the Online Safety Group will assist the Online Safety Coordinator with:

• The production, review and monitoring of the school online safety policy and documents.
• Mapping and reviewing the online safety provision, ensuring relevance, breadth and progression.
• Monitoring network, internet and incident logs.
• Monitoring ‘Whisper’ reports from the school website.
• Consulting parents, carers and pupils about online safety provision.
• Monitoring improvements and actions identified through the 360 degree safe review tool.

Pupils:
• Are responsible for using the school technical systems in accordance with the Pupil Acceptable Use Policy.
• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. This includes using the ‘Whisper’ button on the school website to report incidents from home if they do not feel they can talk to an adult about the issue.
• Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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.

Parents / 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 parent’s evenings, newsletters, website and information about national, local safety campaigns. 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 and applying parental controls on their children’s personal devices.

Community Users/Students
• Community Users and Students who have access to the school systems, internet and VLE will be expected to sign the Adult Acceptable Use Statement before being provided with access to school systems.

Policy Statements
Education – Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. Although technical solutions are a key element within our school, we also recognise the need for a balanced method that includes educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school’s online safety provision. Children and young people will be taught to recognise and avoid online safety risks and build their resilience. Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The computing curriculum is broad, relevant and provides progression. It will be provided in the following ways:

- Pupils should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices.
- Pupils should be supported in building a resilience to radicalisation by providing a safe environment for debating issues and helping them to understand how they can influence and participate in decision making.
- A planned Online safety unit of study is incorporated into the Computing curriculum map for all year groups and should be regularly revisited and identified in planning for all lessons using the internet.
- Key online safety messages will be reinforced during Term 3 Unit of Learning and during Internet Safety day each year. (February)
- Rules for use of the internet will be displayed on laptop and tablet trollies as a visual reminder.
- In lessons where the internet is pre planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material that is found in internet searches.
- It is accepted that from time to time, upper phase children, for good educational reasons may need use search engines without the class teacher providing given websites. Staff must identify this in planning and ensure guidance is given before the occasion. Pupils must not complete this out of the classroom and away from a member of staff.

**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 online behaviours. Parents may underestimate how often children and young people come across potential 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 newsletters, school website
- Parents/Carers sessions
- High profile events and campaigns including Safer Internet Day
- Reference to relevant websites

**Education – The Wider Community**

The school will provide opportunities to share online safety knowledge and experience. This may be offered through the following:

- Providing family learning sessions in online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- The school will share the expertise of our Network Manager to support and advise of any online safety issues on personal devices.
Education & Training – Staff/Volunteers
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 e-safety training will be embedded into the school inset timetable. An audit of the online safety training needs of all staff will be carried out regularly.
• All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
• The Online Safety Coordinator will receive regular updates through attendance at SWGfL, LA or other information and training sessions and by reviewing guidance documents released by others.
• This online safety policy and its updates will be presented to and discussed by staff in staff, phase team meetings, business meetings and INSET days as required.
• The Online Safety Coordinator will provide advice and training as required to individuals as required.

Training – Governors
Governors should take part in online safety training with particular importance for those who are members of the Online Safety Committee. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
• Participation in school training or information sessions for staff or parents.

Curriculum
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of any computing equipment across the curriculum.

• In lessons where internet use is pre-planned, it is best practice that pupils 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.
• Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, teachers may need to demonstrate and research topics that would normally result in internet searches being blocked. In such a situation, staff can temporarily pass the proxy, to remove filters, from their classroom PC’s. This access is for staff demonstration only and closed down immediately after use.
• Pupils should be taught in all lessons to be critically aware of the 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.

Technical – infrastructure, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure 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 ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
• There will be regular reviews and audits of the safety and security of school ICT systems.
• Servers, wireless systems and cabling will be securely located in School Server Room, which is locked at all times.
• All adults have unique user names and passwords, with limited access rights dependent upon need.
  Details of the access rights available to groups of users is recorded by the ICT Technician and kept securely. (see Appendix 1)
• All pupils are provided with a username that begins with a two-digit number that identifies their year of entry into Year 1 followed by their Christian name and initial letter of their surname. Pupils have limited access to the server and are not given passwords.
• The “administrator” passwords for the school ICT system, used by the ICT Technician must also be available to the Online Safety Coordinator and the Head teacher.
• Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
• The ICT technician 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.
• The school maintains and supports the managed filtering service provided by SWGfL.
• Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband of filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
• The school provides an enhanced and differentiated user level of filtering. This enables teaching staff to bypass the proxy to allow access to internet sites (for teaching) that would otherwise be filtered.
• Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.
• Any filtering issues should be reported immediately to SWGfL. An Incident Report Form will be completed. (See copy in Appendix 3)
• The School ICT technician will regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
• An agreed procedure is in place for the provision of temporary access of “guests” (eg student teachers, visitors) onto the school system. (See Appendix 4)
• Only the ICT Technician can download executable files on domain computers.
• Staff, pupils and other users are made aware, when signing the Hardware & Internet Use Statement, that this applies also on laptops and other portable devices provided by school that are intended for use outside the school environment.
• Staff are made aware that removable media (eg memory sticks, CDs, DVDs) should not be used, if not encrypted, to carry any Personal Data. The school provides a secure VPN connection to the school network, accessible from school staff laptops.
• An agreed policy is in place for the use of personal mobile phones whilst on school premises.
• The school infrastructure and individual workstations are protected by up to date virus software.
• Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images
Staff and pupils need to be aware of the risks associated with sharing images and 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 carrying 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. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or local press.
- Staff 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 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 students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. (This is covered in the Parent Permission Booklet, and resigned at the of each academic year.)
- In accordance with guidance from the Information Commissioner’s Office, parents or carers are welcome to take videos and digital images of their children at school for their own personal use. To respect everyone’s privacy and in some cases protection, these images are not to be published or made publicly available on social networking sites nor should parents or carers comment on any activities involving other pupils in digital or video images. This message is reinforced on programmes for school events and through introductions to school performances.
- All digital and video images should be saved into the Media Server in clearly labelled folders. Staff should not keep images in their personal drives or any other storage areas. Staff are allowed to transfer images into the Pupils and Resources Servers to enable access for pupils and themselves, for limited time periods, to allow for access and manipulation. Once completed these images should be deleted or returned to the Media Server.
- This guidance links with the Data Protection Policy which should be read for any clarification.

Data Protection
At Shakespeare Primary School data is recorded, processed, transferred and made available according to the Data Protection Act 1998. This Policy links with our Data Protection Policy which was agreed in 13th October 2016 and is to be reviewed by the HR & Safeguarding Committee in Autumn 2018.

Safeguarding
Shakespeare Primary School is committed to safeguarding and promoting the welfare of all its pupils. This policy links with our Safeguarding Policy and should be read in parallel if required.

Communications
A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:
- Every member of staff is allocated a school email address that can be regarded as safe and secure.
• Users need to be aware that email communications may be monitored.
• Users must immediately report to the Online Safety Coordinator, Phase Leader or Head Teacher as appropriate, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
• Any digital communication between staff and students, pupils or parents, carers (email, chat, VLE 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 public chat, including social networking programmes must not be used for these communications.
• Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
• Pupils should be taught about the safety issues of any digital communications, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate digital communications and be reminded of the need to communicate clearly and correctly and not include any unsuitable or abusive material.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
• Guidance for mobile phone technology use within the school grounds and outside when on trips or meetings is covered in our Mobile Phone Policy and should be read in conjunction with this policy for full details.

**Social Media**
This Policy links with our Social Media Policy which was agreed in October 2012 and is to be reviewed in Summer 2017.
### Unsuitable and 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

**User Actions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Acceptable</th>
<th>Acceptable at certain times</th>
<th>Unacceptable</th>
<th>Unacceptable and illegal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users shall not visit Internet sites, make, post, download, upload,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data transfer, communicate or pass on material, remarks, proposals or</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>comments that contain or relate to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Child sexual abuse images – The making, production or distribution of</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>indecent images of children. Contrary to The Protection of Children Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1978</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Possession of an extreme pornographic image (grossly offensive,</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>disgusting or otherwise of an obscene character) Contrary to the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal Justice and Immigration Act 2008</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Criminally racist material in UK – to stir up religious hatred (or</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>hatred on the grounds of sexual orientation) - contrary to the Public</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Order Act 1986</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pornography</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Promotion of any kind of discrimination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>threatening behaviour, including promotion of physical violence or</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>mental harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Promotion of extremism or terrorism</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Any other information which may be offensive to colleagues or breaches</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>the integrity of the ethos of the school or brings the school into</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>disrepute</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Using school systems to run a private business</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Using systems, applications, websites or other mechanisms that bypass</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>the filtering or other safeguards employed by the school / academy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infringing copyright</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Revealing or publicising confidential or proprietary information (eg</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>financial / personal information, databases, computer / network access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>codes and passwords)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creating or propagating computer viruses or other harmful files</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | X
---|---
On-line gaming (educational) (e.g Mathletics) | x
On-line gaming (non-educational) | x
On-line gambling | x
On-line shopping / commerce (e.g acceptable by school administrators for school purchases only) | x
File sharing | x
Use of social media | x
Use of messaging apps | x
Use of video broadcasting e.g. Youtube | x

**Responding to incidents of misuse**

Shakespeare Primary School uses SWGFL BOOST that includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through responding and managing reported incidents. All members of the school community will be responsible users of digital communication, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

**Illegal Incidents**

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 Flowchart in Appendix 2.

**Other Incidents**

Any incidents that involve inappropriate, but not illegal misuse will be dealt with as soon as possible in a proportionate manner, and that members of the school community will be aware they have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as identified in Appendix 5 and 6.

If the content being viewed 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.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- Have more than one senior member of staff/volunteer involved in the 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 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.)
• 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 actions will be required and could include the following:
  o Internal response or discipline procedures
  o Involvement by the local authority
  o Police involvement and/or action.
## Appendix 1

Access Rights to Shakespeare Primary School Computer System.

<table>
<thead>
<tr>
<th>Role</th>
<th>Child Protection Folder on T Server</th>
<th>Server</th>
<th>Admin Folder</th>
<th>Staff Shared Drive</th>
<th>Media Drive</th>
<th>Resources Drive</th>
<th>Named Drive</th>
<th>Pupils</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT Technician</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Admin Staff</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Teaching Staff</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Head Teacher, Deputy Head Teacher, Senior Leadership Team,</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Parent Support Advisor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pupils</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Guests – Student Teachers on Placement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Guests – Supply Teachers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Guests – Other (i.e Governors, Learning Mentors)</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Appendix 2

Illegal Incidents
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 for responding to online safety incidents and report immediately to the police.
Appendix 3

Copy of the:

**Shakespeare Primary Online Safety Incident Report Sheet**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Person completing sheet)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of person incident relating to</th>
<th>Staff/Pupil/Visitor</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Location/Environment incident took place (i.e. In teaching session/Club/Lunch Time/Home etc)</th>
<th>Date of Incident</th>
</tr>
</thead>
</table>

**Incident Details**

**Reason Why Concern**

**Action Proposed/Taken**

(Please expand and give details taken)

<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
</table>

**Phase Leader Signature**

Cyberbullying/Misuse/Sexting/Other.

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
</table>

Identify type of concern: (tick appropriate box)

<table>
<thead>
<tr>
<th>Cyberbullying</th>
<th>Misuse</th>
<th>Sexting</th>
<th>Other</th>
</tr>
</thead>
</table>

**Online Safety Response to Concern**

<table>
<thead>
<tr>
<th>Online Safety Coordinator received by (date)</th>
</tr>
</thead>
</table>

**Further Action**

<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
</table>

17
Appendix 4

A procedure for the provision of temporary access to ‘guests’ onto the school system.

- Temporary guests sign the Adult Acceptable Internet Use Statement.
- The ICT Technician will provide access rights accordingly. (See procedure for Access Rights – appendix 1)
- Accounts are suspended via active directory after use by the ICT Technician.
- Passwords are regularly changed and subject to the password policy.
Appendix 5

A procedure of sanctions for the misuse of Internet by pupils.

**Pupils**

<table>
<thead>
<tr>
<th>Incidents:</th>
<th>Refer to class teacher / ICT Coordinator</th>
<th>Refer to Phase Team Leader</th>
<th>Refer to Headteacher</th>
<th>Refer to ICT Technician for action re filtering/security etc</th>
<th>Inform parents / carers</th>
<th>Removal of network / internet access rights</th>
<th>Warning</th>
<th>Further sanction eg detention / exclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>√ Action Taken</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P Possible Action Taken</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised use of non-educational sites during lessons</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised use of mobile phone / digital camera / other handheld device</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised use of social networking / instant messaging / personal email</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised downloading or uploading of files</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowing others to access school network by sharing username and passwords</td>
<td>√</td>
<td></td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attempting to access or accessing the school network, using another student’s / pupil’s account</td>
<td>√</td>
<td></td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attempting to access or accessing the school network, using the account of a member of staff</td>
<td>√</td>
<td>√</td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corrupting or destroying the data of other users</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continued infringements of the above, following previous warnings or sanctions</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions which could bring the school into disrepute or breach the integrity of the ethos of the school</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using proxy sites or other means to subvert the school’s filtering system</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accidentally accessing offensive or pornographic material and failing to report the incident</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliberately accessing or trying to access offensive or pornographic material</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix 6

### Staff Incidents

<table>
<thead>
<tr>
<th>Incidents</th>
<th>Refer to Headteacher</th>
<th>Refer to Local Authority / HR</th>
<th>Refer to Police</th>
<th>Refer to Technical Support Staff for action re filtering etc</th>
<th>Warning</th>
<th>Suspension</th>
<th>Disciplinary action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Unauthorised downloading or uploading of files</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Careless use of personal data eg holding or transferring data in an insecure manner</td>
<td>✓</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Deliberate actions to breach data protection or network security rules</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Corrupting or destroying the data of other users or causing deliberate damage to hardware or software</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>P</td>
</tr>
<tr>
<td>Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>P</td>
<td>✓</td>
</tr>
<tr>
<td>Actions which could compromise the staff member's professional standing</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Actions which could bring the school into disrepute or breach the integrity of the ethos of the school</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Using proxy sites or other means to subvert the school’s filtering system</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Accidentally accessing offensive or pornographic material and failing to report the incident</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Deliberately accessing or trying to access offensive or pornographic material</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>P</td>
</tr>
<tr>
<td>Breaching copyright or licensing regulations</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Continued infringements of the above, following previous warnings or sanctions</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>