Foxmoor Primary School

E-Safety Policy

N. Maycock July 2016

Contents

Appendices:

Those items highlighted in red are currently under review or discussion.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *Headteacher and SMT;*
- *E-Safety Officer;*
- *Staff – including Teachers, Support Staff, Technical staff;*
- *Governors;*
- *Parents.*

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body at the full GB meeting on:	October 22nd 2013
The implementation of this e-safety policy will be monitored by the:	E-Safety Committee
Monitoring will take place at regular intervals:	Annually in September, before the first full GB Meeting
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents)	In July, at the end of each academic year or when a serious breach of the policy occurs:
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.	The next anticipated review date will be September 2014
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	The Local Authority (LA) Safeguarding Officer, Internet Provider, Police, Social Services.

The school will monitor the impact of the policy using:

- logs of reported incidents;
- monitoring logs of internet activity (including sites visited);
- internal monitoring data for network activity;
- surveys / questionnaires of:
    - pupils
    - parents / carers
    - staff;

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. **The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data** (see appendix). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Sub Committee receiving regular information about e-safety incidents and monitoring reports. E-Safety is part of the role of the Child Protection Governor..

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator;
- regular monitoring of e-safety incident logs;
- regular monitoring of filtering / change control logs;
- reporting to relevant Governors meeting.

Headteacher and Senior Leaders

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- **The Headteacher and all other members of the Senior Management Team (SMT) are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).

  SWGfL BOOST includes an 'Incident Response Tool' that steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. This can be downloaded at http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool
- The Headteacher and SMT are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

  SWGfL BOOST includes access to unlimited online webinar training – further details are at http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development
- The Headteacher 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer:

- leads the e-safety committee;
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and other documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with the Local Authority and Governing Body (GB);
- liaises with school technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

  (examples of suitable log sheets may be found later in this document). SWGfL BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents

  (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper)
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant meeting / committee of Governors;
- reports regularly to Senior Management Team;
- the investigation, action and sanctions will be the responsibility of the Headteacher in consultation with the E-Safety Co-ordinator.

Network Manager / Technical staff

We recognise that though the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures as suggested below. It is also important that the managed service provider is fully aware of the school e-safety policy and procedures.

The Network Manager, Technical Staff, Co-ordinator for ICT/Computing is responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack;**
- **that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply;**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;**
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person *(see appendix "Technical Security Policy" for good practice);*
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the network, internet, Virtual Learning Environment (VLE), remote access, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher, E-Safety Officer or SMT for investigation, action or sanction;
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);**
- **they report any suspected misuse or problem to the Headteacher, Senior Leaders or E-Safety Officer for investigation, action or sanction;**
- **all digital communications with students, pupils, parents or carers are on a professional level and only carried out using official school systems;**
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the e-safety and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- 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.

The Designated Safeguarding Lead (DSL)

The DSL will be trained in e-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.

E-Safety Committee

The E-Safety group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and monitoring of the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Group will assist the E-Safety Officer with:

- the production, review and monitoring of the school e-safety policy and associated documents;
- the production, review and monitoring of the school filtering policy and requests for filtering changes;
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression;
- monitoring network, internet and incident logs;
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision;
- monitoring improvement actions identified through use of the 360 degree safe self-review tool. *

*See Appendix

Pupils:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (AUP);**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras; they should also know and understand policies on the taking / use of images and on cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, Virtual Learning Environment (VLE) and information about national or local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website / VLE and on-line pupil records;
- their children's personal devices in the school (where these are allowed).

Community Users

Community Users who access school systems, website or VLE as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement AUA 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. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum (in consultation with the new National Curriculum for Computing 2014) is broad, relevant, provides progression, with opportunities for creative activities and will be provided in the following ways:

- **a planned e-safety curriculum will be provided as part of Computing, PHSE and other lessons and is regularly revisited;**
- **key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities;**
- **in all lessons pupils will be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information;**
- **pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;**
- pupils must understand the need for the Pupil Acceptable Use Agreement (PAUA) and adopt safe and responsible use both within and outside school;
- Staff must act as good role models in their use of digital technologies, the internet and mobile devices;
- 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, 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, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) should temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities;
- letters, newsletters, web site, VLE;
- parents / Carers evenings and sessions;
- high profile events / campaigns e.g. Safer Internet Day;
- reference to the relevant web sites and publications.

e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

(see appendix for further links / resources)

Education – The Wider Community

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

- providing family learning courses in use of new digital technologies, digital literacy and e-safety;
- E-Safety messages targeted towards grandparents and other relatives as well as parents;
- the school website will provide e-safety information for the wider community;
- supporting community groups eg Early Years Settings, Childminders, youth, sports, voluntary groups to enhance their e-safety provision (i.e. supporting the group in the use of Online '*Compass'*, an online safety self-review tool - *www.onlinecompass.org.uk).*

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **a planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly*;***

  SWGfL BOOST includes unlimited online webinar training for all, or nominated, staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development) .
- **all new staff must receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements (AUA);** SWGfL BOOST includes an array of presentations and resources that can be presented to new staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources)
- *the E-Safety Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;*
- *the E-Safety policy and its updates will be presented to and discussed by staff at the regular staff meetings and at focussed training meetings /days;*
- *the E-Safety Officer (or other nominated person) will provide advice, guidance and training to individuals as required.*

Training – Governors

Governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology, e-safety, health and safety, child protection. 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 and information sessions for staff or parents (this may include attendance at assemblies or lessons).

Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school E-Safety Policy and Acceptable Use Agreements. The school will also address the Local Authority policies on these technical issues.

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the those named in the above sections are effective in carrying out their e-safety responsibilities:

As we have changed the school internet provider, we will have different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff: technical, educational and administrative before these revised statements are agreed and added to the policy)

A more detailed Technical Security Policy can be found in the appendix.

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;**
- **there will be regular reviews and audits of the safety and security of school technical systems;**
- **servers, wireless systems and cabling must be securely located and physical access restricted;**
- **all users will have clearly defined access rights to school technical systems and devices.**
- **all users** in Years 5 and 6 **will be provided with a username and secure password** by Mrs j Ravenhill who will keep an up to date record of users and their usernames. **Users are responsible for the security of their username and password. Younger pupils have an individual log on with a group password. See Appendix**
- **the " administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)**
- **The service provider (Connexus) 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.**
  (*We are aware that Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)*
- **internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband and the filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
  There is a clear process in place to deal with requests for filtering changes *(see appendix for more details)*
- The school has provided differentiated user-level filtering allowing different filtering levels for different groups of users – administration staff, teaching staff and pupils.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement..
- An appropriate system is in place for users to report any actual or potential technical incident, or security breach to the Headteacher or E-safety Officer, as agreed.
- The service provider ensures that aappropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place *(to be reviewed)* for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place (to be reviewed) regarding the extent of personal use that users: staff students, pupils, community users and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place (to be reviewed) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place (to be reviewed) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* (see School Personal Data Policy in the appendix for further detail)

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to us implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy must be in place and reference made within all relevant policies before we move forward with this. (see appendix for more detailed BYOD Policy suggestions)

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- **Where possible these devices will be covered by the normal filtering systems, while being used on the premises???**
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- Having discussed the guidance from the Information Commissioner's Office and the Data Protection Act, the governors have decided that only school staff or authorised photographers will be permitted to take videos and digital images of children at school events. This is to respect everyone's privacy and in a number of cases protection; these authorised images will not be published without the parents' permission nor will they be made publicly available on social networking sites, nor should parents / carers share or reproduce any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. These images must only be taken on school equipment, the personal equipment of staff must not be used for such purposes.
- Care must be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- 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 as part of the AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix)*
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection;

The school must ensure that:

- **it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes for which it was collected;**
- **every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;**
- **all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" (**see Privacy Notice section in the appendix);
- **it has a Data Protection Policy** (see appendix for policy);
- **it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);**
- responsible persons are appointed Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs);
- risk assessments are carried out;
- it has clear and understood arrangements for the security, storage and transfer of personal data;
- data subjects have rights of access and there are clear procedures for this to be obtained;
- there are clear and understood policies and routines for the deletion and disposal of data;
- there is a policy for reporting, logging, managing and recovering from information risk incidents;
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- **take care to ensure the safe keeping of personal data at all times , minimising the risk of its loss or misuse;**
- **use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;**
- **transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected';
- the device must be password protected **NOTE:** *many memory sticks / cards and other mobile devices cannot be password protected';*
- the device must offer approved virus and malware checking software';
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

(We will need to review our policy as to whether data storage on removal media is allowed, even if encrypted – -some organisations do not allow storage of personal data on removable devices.)

The Personal Data Handling Policy Template in the appendix provides more detailed guidance on the school's / responsibilities and on good practice.

Communications

Currently only in exceptional circumstances are pupils permitted to bring a mobile phone to school. Parents apply to the Headteacher for such permission and, if granted, the phone is kept securely in the school office during the day. Any phone brought to school without this permission is confiscated.
However, our duty is to embrace new technologies and teach children how to use them safely this is a dilemma we need to address.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

We will need to discuss and agree how we intend to implement and use these technologies e.g. allowing pupils to use mobile phones/tablets BYOD in lessons. This section may also be influenced by the age of the pupils. The table has been left blank so that we can decide our responses.

	Staff & other adults				Pupils			
Communication Technologies	Allowed	ed at certain times	d for selected staff	Not allowed	Allowed	ed at certain times	with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones / cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

We may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

When using communication technologies the school considers the following as good practice:

- the official *school* email service may be regarded as safe and secure and is monitored; users should be aware that email communications are monitored;
- *staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access);*

- in accordance with the school policy, users must immediately report, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, to the nominated person, and must not respond to any such communication);
- any digital communication between staff and 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 social media must not be used;
  - ***Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use (or shall we choose to use group or class email addresses for younger age groups in KS2?);*
  - *Pupils must be taught about e-safety issues, such as the risks attached to the sharing of personal details;*
  - *Pupils must also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;*
  - *Personal information must not be posted on the school website and only official email addresses must be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

  SWGfL BOOST includes unlimited webinar training on this subject: (*http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development*)
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

School staff must ensure that:

- no reference is made in social media to pupils, parents / carers or school staff;
- they do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions must not be attributed to the school or local authority;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Senior Risk Officer and E-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

***** For discussion and decision***

SWGfL BOOST includes SWGfL alerts that highlight any reference to the school in any online media (newspaper or social media) for example http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Alerts

Unsuitable / inappropriate activities

Internet activity such as accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. Below is a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those 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 usage as follows:

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

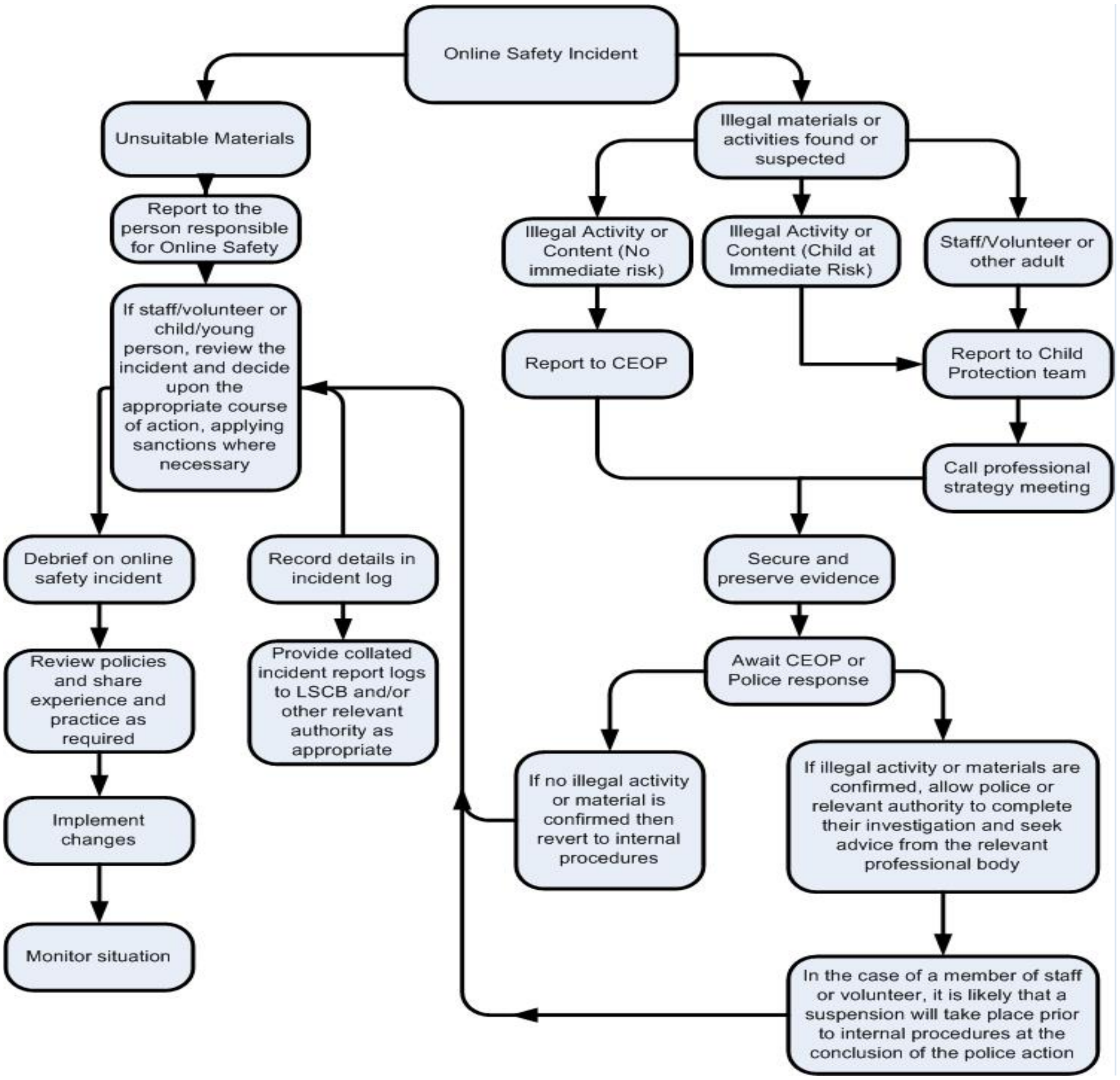
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above*).*

SWGfL BOOST includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through how to respond, forms to complete and action to take when managing reported incidents (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

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 (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

•

Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed.

- Have more than one senior member of staff involved in this process: this is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise; use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by Local Authority or national organisation (as relevant).
  - police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures as follows:***

***** In the light of the changes to the National Curriculum for ICT in 2014 we will need further discussion to agree upon our responses and possibly place the ticks in the more relevant columns. We may also wish to add additional text to the column(s) on the left to clarify issues. We will use the charts below at staff meetings / training sessions.*

Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to E Safety Officer or SMT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning in the first instance and recorded	Further sanctions leading to exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	x	x	X				X
Unauthorised use of non-educational sites during lessons	X	X				X	X	X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X	X	X	X
Unauthorised use of social media / messaging apps / personal email	X	X	X		X	X	X		X
Unauthorised downloading or uploading of files	X	X	X		X	X		X	X
Allowing others to access school network by sharing username and passwords	X	X	X		X	X	X		X
Attempting to access or accessing the school network, using another pupil’s account	X	X	X		X	X	X		X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X		X
Corrupting or destroying the data of other users	X	X	X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X		X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X			X excl
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X		X
Using proxy sites or other means to subvert the school’s filtering system	X	X	X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X		X	

Staff Actions / Sanctions

Incidents:	Refer to E Officer	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning in the first instance to be recorded	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X			X
Inappropriate personal use of the internet / social media / personal email	X	X				X	→	X
Unauthorised downloading or uploading of files	X	X			X	X	→	X
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	X	X				X	→	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X	→	X
Deliberate actions to breach data protection or network security rules	X	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X						X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X			X			X
Actions which could compromise the staff member's professional standing	X	X	X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy	X	X	X					X
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X			X
Breaching copyright or licensing regulations	X	X			X			
Continued infringements of the above, following previous warnings or sanctions	X	X						X

Appendix:

The school is going to apply for the E-Safety award in 2017

We intend to use the following as a benchmark:

360 degree safe E-Safety Self Review Tool

360 degree safe is an online, interactive Self Review Tool which allows school to review the e-safety policy and practice. It is available, free of charge.

Schools choose one of 5 level statements in each of the 28 aspects. The tool provides an "improvement action" describing how the school might move from that level to the next. Users can immediately compare their levels to the benchmark levels of all the schools using the tool. There is a range of reports that they can use internally or with consultants.

The tool suggests possible sources of evidence, provides additional resources / good practice guidance and collates the school's action plan for improvement. Sections of these policy templates can also be found in the links / resources section in 360 degree safe.

Schools that reach required benchmark levels can apply for assessment for the E-Safety Mark, involving a half day visit from an accredited assessor who validates the school's self review. More information about the E-Safety Mark can be found at: http://www.360safe.org.uk/Accreditation/E-Safety-Award

SWGfL BOOST – Schools online safety toolkit

http://boost.swgfl.org.uk/home.aspx

http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies