SPRINGWOOD PRIMARY SCHOOL

Online Safety Policy including Mobile Phone Policy, Acceptable Use Policy and Social Networking Guidance

Headteacher: Mrs. Jacqui Wennington

Headteacher:	Jacqui Wennington
Written / Reviewed by:	Judith Pitt
Date written:	September 2012
Next Review:	March 2025

Using New Learning Technologies Effectively and Safely

Contents

Writing and reviewing the Acceptable Use Policy

The Online Safety Policy relates to other policies including those for Computing, Anti-bullying and Safeguarding.

Springwood's Online Safety Policy has been developed by the school, agreed by senior leadership, and approved by governors.

Safety Audit

This quick self-audit will help the Senior Leadership Team (SLT) assess whether the online safety basics are in place to support a range of activities.

Has the school an Online Safety Policy that complies with national guidance?	Yes
Date of latest update:	November 2020
The policy was agreed by governors on:	27th January 2016
The policy is available for staff at:	Staff shared / Policies
The policy is available for parents/carers	On request
The Designated Safeguarding Leads are:	Judith Pitt / Aidan Yates / Matthew Lawrenson
The Online Safety Coordinator is:	Judith Pitt
Has Online Safety training been provided for both pupils and staff?	Ongoing
Do all staff, including supply staff, sign an ICT Code of Conduct on appointment?	Yes
Do parents/carers sign and return an agreement that their child will comply with the school Online Safety Rules?	Yes
Have school Online Safety Rules been set for pupils?	Yes
Are these rules displayed in all rooms with computers, in a form accessible to all pupils?	Yes
School internet access is provided by an approved educational internet service provider and complies with DfE requirements for safe and secure access.	Yes
The school is aware of the nature of the internet filtering policy applied to its network by its provider.	Yes
Is this policy understood by all staff and has it been approved by SLT?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes
Should an incident take place the Online Safety Incident flowchart should be followed.	Appendix 2

Scope of this Policy

The School Online Safety Policy applies to all members of the school community including staff, pupils, volunteers, parents / carers, visitors and community users who have access to and are users of Springwood's ICT systems and mobile technologies both in and out of school.

The purpose of this policy is to provide the staff of Springwood Primary School with appropriate procedures for the protection or safeguarding of children when interacting with the internet on a daily basis and experience a wide range of opportunities, attitudes and situations.

Online Safety covers issues relating to children as well as adults and their safe use of the internet, mobile phones, iPads and other electronic communications technologies, both in and out of school. It includes education for all members of Springwood on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Springwood must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. All members of staff need to be aware of the importance of good online safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an Online Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider community.

Roles and Responsibilities

Governors

- Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness.

Head Teacher and Senior Leaders

- The Head Teacher is responsible for ensuring the safety (including online safety) of staff and pupils.

- The Head Teacher and other members of the Senior Leadership Team are 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

At Springwood the role of Online Safety Coordinator is combined with that of the Safeguarding Coordinator. The coordinator is responsible for:

- taking day to day responsibility for online safety issues and having a leading role in establishing and reviewing the school's policy.

- ensuring that all members of staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;

- providing training and advice for staff;

- holding a log of online safety incidents to inform future Online Safety developments.

Network Manager

The school's network manager, Virtue, is responsible for ensuring that:

- Springwood's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Springwood meets the Online Safety technical requirements as outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety policy and guidance;
- users only access the Springwood networks through a properly enforced password protection policy.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that they:

- have an up-to-date awareness of online safety matters and of the current Springwood Online Safety policy and practices;
- have read, understood and signed the Springwood Staff Acceptable Use Policy;
- report any suspected misuse or problem to the Online Safety Coordinator for investigation.

Designated Person for Safeguarding

The Safeguarding Coordinator should be trained in Online Safety issues and be aware of the potential for serious Child Protection issues to arise from:

- sharing personal data;
- access to illegal / inappropriate materials, including extremist material;
- inappropriate online contact with adults / strangers;
- potential or actual incidents of grooming;
- cyberbullying.

Pupils

- Pupils need to understand online restrictions - what they are able to access and what they are not. (Online filters, provided by internet provider, are in place to ensure pupils remain safe online).

Parents / Carers

The school will take every opportunity to help parents / carers understand these issues through Parents / Carers Evenings, letters, and the website. Parents and carers will be responsible for:

- endorsing by signature the Parent / Carer Online Safety agreement form;
- accessing Springwood's ICT systems in accordance with the school's Acceptable Use Policy.

Education and Training – Staff

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

- A planned Online Safety introduction included during new staff induction and acceptable use form signed.

- All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand Springwood's Online Safety policy, Acceptable Use Policies and Guidelines.

Teaching and Learning

Why internet use is important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of internet use in Springwood is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance Springwood's management functions.

How does internet use benefit education:

Benefits of using the internet in education include:

- access to worldwide educational resources including museums and art galleries;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;

Pupils will be taught how to evaluate internet content, where appropriate.

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what internet use is responsible and what is not and given clear objectives for internet use, appropriate to their understanding.

- Pupils on the formal curriculum pathway learn about online safety through the E-Aware programme.

- Any specific online safety issues that may arise are addressed with the pupil(s) concerned, their peers (as appropriate), and parents / carers, eg harmful online challenges and online hoaxes; inappropriate content that pupils are uploading on to YouTube.

Managing Internet Access

Information system security:

- Springwood's ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the managed service and Local Authority.

Managing filtering:

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator and the managed service will be informed so that they can take appropriate action.

See Appendix 3 for further information about filtering.

Staying safe

The school will ensure that pupils and parents are aware of online safety issues. The pupils will be taught about online safety through Computing and E-Aware sessions and reminded about the expectations as appropriate.

- The school internet access is designed expressly for pupil use and includes appropriate filtering.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.

Published content and the school website

Any information that can be accessed on the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupil's full names will not be used anywhere, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or video of pupils are published, e.g. on the school website.
- Where pupil's work is published the school will ensure that the child's identity is protected.

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) 2018.

Policy Decisions

Authorising internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted internet access.
- Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- User IDs and passwords must not be shared, nor should any user allow anyone else to browse the internet using their ID, in accordance with the corporate password policy of Salford City Council.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Salford LA can accept liability for the material accessed, or any consequences of internet access. Any inappropriate access, including access to extremist material, whether intentional or unintentional will be reported to the Online Safety co-ordinator and to the LA where necessary.
- The school will audit ICT provision to establish if the Acceptable Use Policy is adequate and that its implementation is effective.
- SOPHOS is the internet filtering system used in school.

Handling Online Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff and, where appropriate, the LA will be informed.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure on request.

Communicating the Policy

Introducing the Online Safety policy to pupils

- Visual Online Safety rules will be posted in all networked rooms and discussed with the pupils, where appropriate.

Staff and the Acceptable Use Policy

- All staff will be given the school Acceptable Use Policy and its importance explained.
- Staff will be informed that network and internet traffic can be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school and managed service will use monitoring software to ensure that inappropriate materials, including extremist material, are not being stored or used on school equipment.

Enlisting parents' support

- Parents may have a copy of the Acceptable Use Policy on request.
- The school will ask all new parents to sign the parent / pupil agreement as part of the admissions meeting.

Remote Learning

Due to the Covid pandemic, pupils are spending extended periods of time at home and appropriate learning activities are provided at these times. Zoom calls are used in some cases to keep in touch with parents, communicate about their child's progress and, occasionally, to communicate with the pupil alongside their parent. In order to keep pupils, parents and staff safe, we have rules for Zoom calls for both staff and parents. These can be found in the Home Learning Policy.

This policy should be read alongside the Safeguarding Policy and Home Learning Policy.

Springwood Primary School

Mobile Phone Policy

Introduction.

1.1 Mobile phone technology has become more sophisticated over recent years and will continue to evolve. Wireless connections in particular are to extend the capabilities of mobile phones further which will allow access to new content and services, such as the internet, social networking sites and instant messaging. Many mobile phones offer camera, video and audio recording as standard.

1.2 Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance, however, as with any other form of technology, there are to be associated risks. Children and young people must be encouraged to understand such risks to enable them to develop the appropriate strategies which will keep them safe.

1.3 As with online safety issues generally, risks to children and young people should be broadly categorised under the headings of:

- Content
- Contact
- Conduct
- Commerce

These issues are to be managed by reducing availability, restricting access and increasing resilience.

1.4 This philosophy is to be applied to the use of mobile phones through the Mobile Phone Policy. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses as to be agreed with the Designated Lead for Safeguarding. Any authorised use of mobile phones is to be monitored and recorded. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

1.5 Under no circumstances are images, video or audio recordings to be made without prior explicit written consent by the Designated Lead for Safeguarding.

1.6 Mobile devices will not be connected to the Springwood Wifi.

2. Aim

2.1 The aim of the Mobile Phone Policy is to protect children and young people from harm, by ensuring the appropriate management and use of mobile phones by all individuals who are to come into contact with pupils.

2.2 Children and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way and to be alert to the potential risks of such use.

2.3 This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

3. Scope

3.1 The Mobile Phone Policy will apply to all individuals who are to have access to and / or be users of personal and / or work related mobile phones within the broadest context of the school. This will include children and young people, parents and carers, school staff, volunteers, students, visitors, contractors and community users. This list is not to be considered exhaustive.

4. Policy statement

4.1 It is to be recognised that it is the enhanced functions of many mobile phones that will give the most cause for concern and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and bullying.

4.2 It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not being considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

4.3 Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others.

4.4 It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

5. Code of Conduct

5.1 A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the children and young people in their care.

5.2 It is to be ensured that all school staff will:

- Be aware of the need to protect children from harm
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk
- Be vigilant and alert to potential warning signs of misuse
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations
- Understand the need for professional boundaries and clear guidance regarding acceptable use
- Be responsible for the self-moderation of their own behaviours
- Be aware of the importance of reporting concerns immediately

5.3 It is to be recognised that studies consistently indicate that imposing rigid regulations and / or 'bans' on the actions of others are counterproductive and should be avoided. Such imposition will lead to a culture of suspicion, uncertainty and secrecy. An agreement of trust is therefore to be promoted regarding the carrying and use of mobile phones. This is to be agreed by all service users.

6. Procedures

6.1 Clearly defined policies and procedures will aim to ensure effective safeguarding practices are in place to protect children from harm and exposure to behaviours associated with misuse. The need to ensure mobile phones will not cause unnecessary and / or unsafe disruptions and distractions in the workplace are also to be considered.

6.2 Acceptable use and management of mobile phones is to be agreed by all staff. There is to be a clear expectation, for example, that all personal use of mobile phones is to be limited to allocated lunch and / or breaks, unless it is to be otherwise agreed by the Designated Lead for Safeguarding. Such authorised use is to be monitored and recorded. Safe and secure storage facilities are available to store personal belongings as necessary.

6.3 The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided except where it is to be explicitly agreed otherwise by the Designated Lead for Safeguarding. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Designated Lead for Safeguarding is to be able to withdraw or restrict authorisation for use at any time if it is deemed necessary. (This also applies to any other personal devices that have imaging and sharing capabilities, eg laptop, iPad.)

6.4 Staff are not to use their own personal mobile phones for contacting children and young people, parents and carers. If it is deemed necessary, it must be with the explicit written consent of both the Designated Lead for Safeguarding and the parent or carer; unless it is considered an emergency.

6.5 All service users, including parents, carers, visitors and contractors should be respectfully advised that their mobile phones are not to be used in school. Should it be considered necessary for mobile phone calls and / or texts to be taken or made, the person will be asked to step outside the building. No images, video or audio recordings are to be made without prior explicit written consent by the Designated Lead for Safeguarding.

6.6 All individuals who are to bring personal devices into school must ensure that they hold no inappropriate or illegal content, including extremist material.

7. Emergency Contact

7.1 It is to be recognised that mobile phones provide direct contact to others and will often provide necessary reassurances due to their ease of access, particularly at difficult times. Agreed acceptable use of mobile phones is therefore promoted. This is to afford staff peace of mind, by reducing stress and worry and is therefore to allow them to concentrate more fully on their work. Such use must be subject to management, monitoring and review.

7.2 It is to be ensured that the landline telephone remains connected and operational at all times, except in circumstances beyond reasonable control. This means that the landline is to be available for emergency / urgent contact at all times.

Mobile Phone Code of Conduct

- Mobile phones are to be stored safely away during the course of the school day. No mobile phones are to be kept on their person by any member of staff (unless agreed by SLT due to exceptional circumstances).

- Mobile phones must be switched off and they should not be used to make or take personal calls / messages during the school working day.

- Staff should not leave the classroom during lessons to use their mobile phones.

- Mobile phones are permitted to be used in the staffroom or outside the school building during allocated breaks.

- Staff wishing to use Facetime / Skype must do so outside the school building.

I have read and understand the Mobile Phone Policy and associated Code of Conduct.

Signed: ..... **Date: .....**

Print Name: .....

Springwood Primary School
Acceptable Use - Staff Code of Conduct for ICT

School Policy

This Acceptable Use Policy is intended to ensure that:

- staff, volunteers, visitors and community users will be responsible users and stay safe while using the internet and other communication technologies for educational, personal or recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- Staff, volunteers, visitors and community users are protected from potential risk in their use of ICT as part of their everyday work.

The school will try to ensure that staff, volunteers, visitors and community users will have good access to ICT to enhance their work, to enhance opportunities for pupils learning and will, in return, expect staff, volunteers, visitors and community users to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way to ensure there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the pupils in my care in the safe use of ICT and embed E-Safety in my work with them.

For my professional and personal safety I understand that:

- the school will monitor my use of the ICT systems, email and other digital communications;
- the rules set out in the agreement also apply to use of Springwood's ICT systems, e.g. laptops, iPads, email, etc, when out of school;
- the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school;
- I will not disclose any username, password or security information to anyone other than an authorised system manager;
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy or remove or otherwise alter any other user's files, without their express permission;
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy and the use of digital / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published, e.g. on the school website, it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policy.

- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- Where school have issued hand held / external devices, eg laptops, iPads, mobile phones, or any other device with imaging and sharing capabilities, I will follow the rules set out in this agreement in the same way as if I were using equipment based in school. I will also follow any additional rules in line with the Online Safety policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from such viruses.

- I will not use any personal devices for school activities apart from taking my mobile phone on educational visits, only for use in an emergency to contact school.

- I will not use personal email addresses on the school ICT systems.

- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.

- I will ensure that any data is regularly backed up in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act, extremist material) or inappropriate or may cause harm or distress to others. I will not try to use programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not install or attempt to install programs of any type on a machine or store programs on a computer nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others as outlined in the School / Local Authority Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that the data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the ICT Technician / School Business Manager.

- I will immediately report any lost equipment to SLT.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I will only use the Springwood Wifi through Springwood designated devices, eg laptops, computers and iPads.

Springwood Primary School
Acceptable Use - Staff Code of Conduct for ICT

This form relates to the Staff Acceptable Use Policy to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and or the Local Authority and, in the event of illegal activities, the involvement of the police.

- I have read and understood Springwood's Online Safety Policy

- I have read and understood the above and agree to use Springwood's ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signature: _____ Date: _____

Full Name: _____ (printed)

Job title: _____

Springwood Primary School
Social Networking Guidelines for Teachers and Support Staff

It has been widely reported that school staff have been prosecuted for inappropriate posts on Social Networking Sites (e.g. Facebook, Twitter, MySpace, etc.)

As a result of this, we are asking that Springwood employees, agency staff, volunteers, students and anyone who comes into contact with the school's email, network or internet services follow these guidelines:

- Set the security settings of your account so that only 'friends' can access your details, pictures and posts.
  Employers, pupils, parents and others will search networking sites looking through lists of 'friends of friends' in order to find who / what they are looking for. 'Friends of friends' and 'networks and friends' open your contents to a large group of unknown people.

- Do not initiate or accept pupils, parents, Governors, school volunteers, or college / university students on placement at Springwood as 'friends.'
  It is important to maintain a professional relationship with these people and to avoid associations that could cause bias in the classroom, impact on the parent / school relationship or bring the school into disrepute.

- Remember that people classified as 'friends' have the ability to download and share your information with others.

- Do not discuss pupils or colleagues or publicly criticise school policies or personnel.
  Be particularly careful not to refer to specific events / incidents that happen in school that may be identifiable by others. Remember that you may have added your place of work to your profile.

- Do not use commentary deemed to be defamatory, obscene, proprietary, or libellous.
  Exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations.

- Do not post pictures of yourself engaging in inappropriate activities.

- A good rule to remember: "Post only what you would like your boss or mother to read."
  Bear in mind that on a social networking site, once you post something it may be available even after it is removed from the site.

Springwood Primary School

Social Networking Guidelines for Teachers and Support Staff

User Signature

I understand that it is my responsibility to ensure that I remain up to date and read and understand the school's most recent Social Networking Guidelines.

I agree to apply these principles to my use of Social Networking Sites.

Signature: _____ Date: _____

Full Name: _____ (printed)

Job title: _____

Springwood Primary School

Parent / Carer Online Safety Agreement Form

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.
If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils are not referred to by name on the video and that pupils' full names are not given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the interactive board in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school
  e.g. in school wall displays and PowerPoint presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a DVD or a document sharing good practice; on the school website. In rare events, your child could appear in the media if a newspaper photographer or television film crew attend an event.

- Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, eg if your child won a competition and wanted to be named in local or national literature.

Springwood Primary School

Parent / Carer Online Safety Agreement Form

Parent / Carer name: _____

Pupil name(s): _____

Parent's Consent for Internet Access:

As the parent or carer of the above pupil(s), I grant permission for my daughter or son to have access to use the **i**nternet and other ICT facilities at school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school will use monitoring software to ensure that inappropriate materials are not being stored or used on school equipment.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety. I understand that staff are asked not to engage with pupils and parents / carers through social networking sites.

Parent's / Carer's Consent for Web Publication of Work and Photographs:

I agree that my son / daughter's work may be electronically published.

I also agree that appropriate images and video that include my son / daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent / Carer signature: _____

Date: ____ **/** ____ **/** ____

(Please delete any statements if you do not agree with them)

Appendix 1

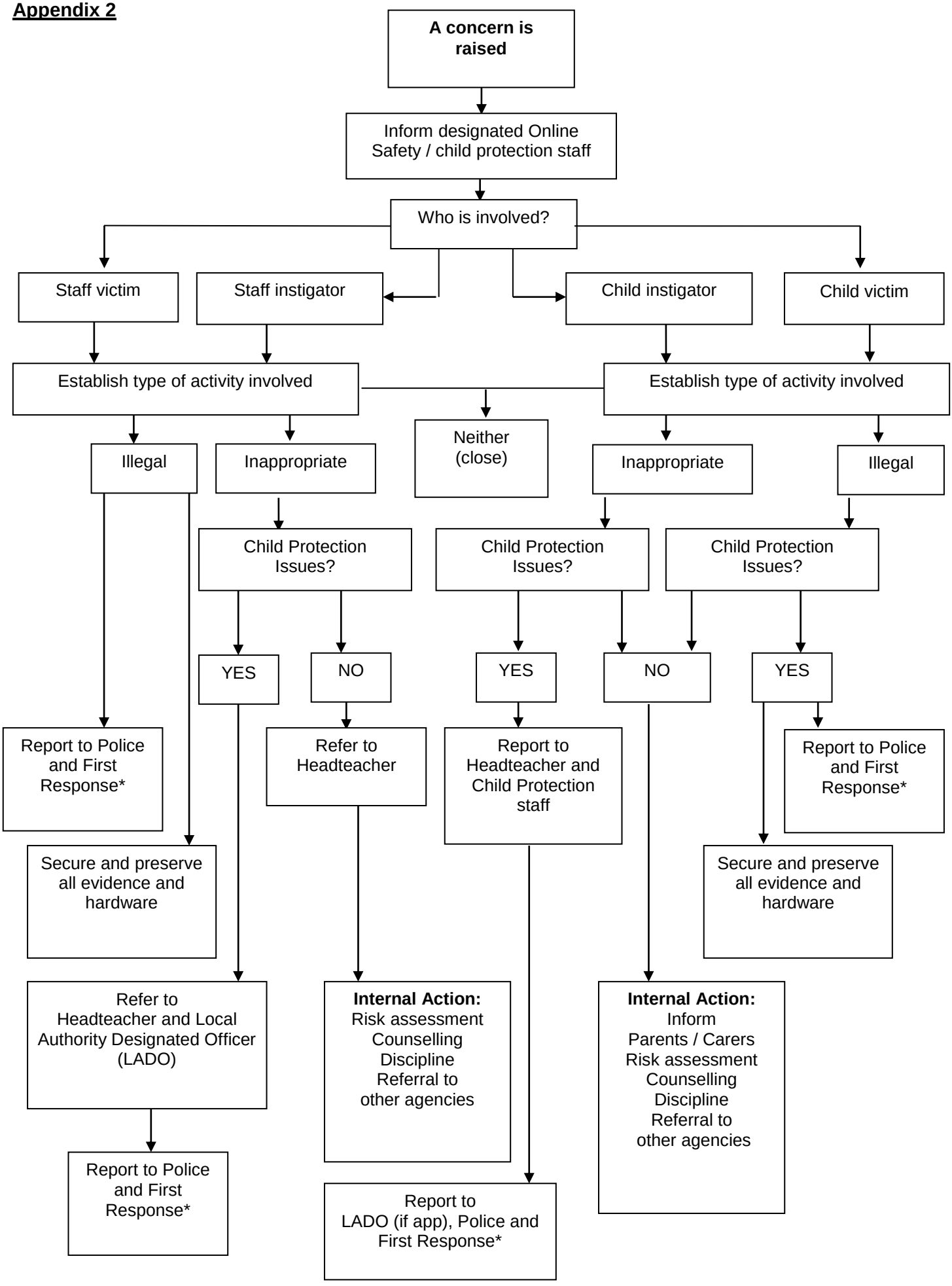
Springwood Primary School
Online Safety Good Practice Guidelines

ICT Device	Best Practice	Safe Practice	Poor Practice
Email	Staff and pupils should only use the school email account for communication with each other.	Check the school Online Safety policy regarding use of your school email or internet for personal use.	Do not use your personal email account to communicate with pupils and their families without the Head Teacher's knowledge or permission and in accordance with the Online Safety policy.
Images, photos and videos	Only use school equipment for taking pictures and videos. Ensure parental permission is in place.	Check the Online Safety policy for instances when personal equipment / devices may be used. Always make sure that you have the Head Teacher's knowledge or permission. Make arrangement for pictures to be downloaded to the school network immediately after the event. Delete images from the camera / device after downloading.	Do not download images from school equipment to your own. Do not use your equipment without the Head Teacher's knowledge or permission and in accordance with the Online Safety policy. Do not retain a copy or distribute images for your personal use.
Internet	Understand how to search safely online and how to report inappropriate content.	Staff should be aware that monitoring software will log online activity. Be aware that keystroke monitoring does just that – your passwords, credit card numbers and security codes will be visible to the monitoring technicians.	Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings.
Mobile Phones	Follow the school policy and guidelines re use of mobile telephones.	Check the Online Safety policy for any instances where using your personal phones may be allowed. Staff make sure you know how to employ safety measures such as concealing your number by dialling 141 first.	Do not use your own phone without the Head Teacher's knowledge or permission. Do not retain pupil or parental contact details for your own personal use.

ICT Device	Best Practice	Safe Practice	Poor Practice
Social Networking	If you have a personal account regularly check all settings and make sure your security settings are not open access. Ask family and friends to not post tagged images of you on their open access profiles.	Do not accept people you do not know as friends. Be aware that belonging to a group can allow access to your profile.	Do not have an open access profile that includes inappropriate personal information and images, photographs or videos. Do not accept pupils or their parents as friends on your personal profile. Do not accept ex-pupils as friends. Do not write indiscreet posts about colleagues, pupils or their parents.
Webcams	Make sure you know about inbuilt software / faculties and switch off when not in use.	Check the Online Safety policy for any instances where using personal equipment may be allowed. Always make sure that you have the Head Teacher's knowledge or permission. Make arrangements for pictures to be downloaded to the school network as soon as possible after the event. Delete images from the camera / device after downloading.	Do not download images from school equipment to your own. Do not use your own equipment without the Head Teacher's knowledge or permission and in accordance with the Online Safety policy.

Online Safety Incident Flowchart

Appendix 2



Appendix 3

Providing a Safe Environment for our Internet Customers – Virtue Technologies

Introduction
Virtue Technologies is committed to providing a reliable and safe internet service that meets the ongoing needs of schools to provide a safe environment for their students. Our services are fully aligned to the Internet Watch Foundation (IWF) guidelines and our service partners (Talk Talk Business, Virgin Media, Sophos and Impero) are full IWF members as recommended by the UK Safer Internet Centre and the Department for Education.

Filtering
In line with the Internet Watch Foundation, our Internet service is designed to ensure that our customers are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering. Our filtering solution is based on the Sophos Security Gateway and provides a robust internet filter with automated updates to inappropriate sites, including the IWF blocked sites list.

Illegal online content
We ensure that access to illegal content is blocked in line with:

- the IWF block list
- block access to illegal Child Abuse Images and Content (CAIC) and
- 'the police assessed list of unlawful terrorist content', produced on behalf of the Home Office.

Inappropriate Online Content
We recognise that no filter can guarantee to be 100% effective and we continually work with both our customer schools and industry partners to provide the safest environment possible for our customers.

In addition to the illegally blocked content, we also block content related to:

- Discrimination
- Drugs and Substance abuse
- Malware and hacking
- Pornography
- Piracy and copyright theft
- Self-Harm
- Violence

Our filtering solution, powered by the Sophos Security Gateway, provides the following features:

- Age appropriate, differentiated filtering: Our filtering solution includes the ability to vary filtering strength appropriate to age and role, e.g. teachers and students are frequently configured to use a different filter.
- Control: Our solution has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content.
- Filtering Policy: We publish our rationale that details our approach to filtering with classification and categorisation, as well as what is blocked.
- Identification: Our solution is integrated into the School's Active Directory and has the ability to identify users by their network username.
- Mobile and App content: Our solution is not limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies.
- Network level: Filtering is applied at 'network level' and is not reliant on any software on user devices.
- Reporting: Our solution has the ability to report inappropriate content for access or blocking.
- Reports: Our solution offers clear historical information on the websites visited by users.

Monitoring

Virtue Technologies provides full reporting and log files that contains information relating to each internet website that is visited (including where sites are blocked) through the installed Sophos Security Gateway. In addition to the logging the date, time and user details, these reports also contain other information, such as search term usage against individuals. Logs are stored locally on the Sophos SG and are retained for at least 6 months.

Internet usage reports contain information that will help the school understand how their internet service is being used, such as:

- which users use the internet the most
- attempts to access blocked websites
- requests that try to override the content filter
- top websites being accessed
- performance of the internet circuit

Should an item on the report warrant further investigation, additional reports can be created to gather information on a specific aspect of the service, for example, an individual user's activity or who has accessed a specific website.

Training and Support

To further provide our customers with a safe solution, our internet, filtering and monitoring solutions are only installed and managed by engineers with a high level of training and certification with Sophos. As a minimum, our Engineers attain the qualification of Sophos Certified Engineers.

We provide training to enable customers to make changes to their own internet filtering. However, customer access to the solution does not allow them to open sites blocked on the basis of being illegal. This training is completed when we initially install the solution on site and is backed up by regular (free) training events to maintain our customer's skills.

To help our customers with complex filtering changes or where the customers does not have the confidence to make changes themselves, our Support Team are on hand to provide assistance and unblock sites for them.