Springfield School

e-Safeguarding Policy

Contents

Introduction

At Springfield School we believe that digital technologies improve and enhance learning at all ages. With thoughtful and imaginative planning, these devices and systems can increase independence and engagement, provide opportunities for different learning styles, and allow learning to be connected from school to home.

Springfield School understands the risks to all members of our community that are inherent in the integration of digital technologies into our learning and teaching. This policy will explain how we are providing the necessary safeguards to help ensure we are doing everything that could reasonably be expected of us to manage and reduce these risks. This policy also addresses wider educational issues in order to help our children, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

Scope of the Policy

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

- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other e-safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

- The school will identify within this policy, and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents / carers of incidents of inappropriate e-safeguarding behaviour that take place out of school.

Development of this Policy

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

- Linda Joseph - Deputy Headteacher/School E-Safety Coordinator
- Joanne Hanney - office manager
- Stephen Cole - teacher
- Representative from Bue Box (ICT technical support)

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- INSET Day on September 1st 2013
- Governors meeting

Schedule for Development / Monitoring / Review

Title:	Springfield School E-Safeguarding Policy
Version:	1.0
Date:	1st September 2013
Author:	Springfield School e-safeguarding working group

Monitoring will take place at least annually or more frequently if occasioned by new technologies or incidents of concern.

The Governing Body will receive a report on the implementation of the policy including anonymous details of any e-safeguarding incidents at least annually.

The 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-safeguarding incidents take place, the LA Safeguarding Officer should be informed.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
    - students / children (including Every Child Matters Survey)
    - parents / carers
    - staff

All staff and members of the School community must be informed of any relevant amendments to the policy.

Communication of the Policy

.

- Springfield School’s senior leadership team will be responsible for ensuring all members of school staff and children are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.
- The eSafeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- The eSafeguarding policy will be introduced to the children at the start of each school year
- The elements of this eSafeguarding policy which pertain to the rights and responsibilities of Springfield children will be included in the ongoing curriculum across the school.
- On the occasion of any amendments to the eSafeguarding policy there will be age related learning for all classes which explains and communicates the changes.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used
- Safeguarding posters will be prominently displayed around the school

Roles and Responsibilities

We believe that eSafeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team:

- The Headteacher has overall responsibility for e-safeguarding all members of the school community, though the day to day responsibility for e-safeguarding will be delegated to the E-Safeguarding Co-ordinator.
- The headteacher and senior leadership team are responsible for ensuring that the eSafeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal eSafeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the eSafeguarding Coordinator.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

Responsibilities of the e-Safeguarding Working Group

- To ensure that the school eSafeguarding policy is current and pertinent.
- To ensure that the school eSafeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

Responsibilities of the e-Safeguarding Coordinator

As at 1st September 2013 - Linda Joseph (Acting Headteacher)

- To promote an awareness and commitment to eSafeguarding throughout the school.
- To be the first point of contact in school on all eSafeguarding matters.
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures.
- To lead the school eSafeguarding working group
- To have regular contact with other eSafeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with school technical staff.
- To communicate regularly with the designated eSafeguarding governor.
- To communicate regularly with the senior leadership team.

- To create and maintain eSafeguarding policies and procedures.
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- To ensure that eSafeguarding education is embedded across the curriculum.
- To ensure that eSafeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on eSafeguarding issues to the eSafeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- To ensure that an eSafeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with children should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide children carefully when engaged in learning activities involving technology.
- To ensure that children are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

As at 1st September 2013 - Blue Box IT Limited, Unit 17, President Buildings, Savile Street East, Sheffield S4 7UQ

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work.

- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, work placement students and volunteers

Communication between adults and between children and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff and volunteers should:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from a child, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- not send or accept a friend request from the child person on social networks.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children in their care (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the school into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Child Protection Officer

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of Springfield children

- To read, understand and keep to Springfield children's Acceptable Use Policy.
- To help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies on the taking and use of mobile phones.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss eSafeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support Springfield School in promoting eSafeguarding.
- To read, understand and promote the Springfield children's Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

To sign a home-school agreement containing the following statements:

- We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community
- We will support the school's stance on the use of ICT and ICT equipment
- Images taken of children at school events will be for personal use only and not uploaded or shared via the internet
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school
- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by children.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages children to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.

The role of the E-Safety Governor includes:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to Governors meeting

Education

Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children 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 education will be provided in the following ways:

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the curriculum.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with children routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Children will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind children about their responsibilities through an end-user Acceptable Use Policy which every child will sign and will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach children how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, children will be guided to use age-appropriate search engines. All use will be monitored and children will be reminded of what to do if they come across unsuitable content.
- All children will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- children will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- children will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

All Staff (including Governors)

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.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This E-Safeguarding policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through

- parents' meetings
- newsletters
- website
- information about national and local e-safety campaigns

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children 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.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children' 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 children are published on the school website as part of the AUP signed by parents or carers at the start of the year (see Parents / Carers AUP Agreement in the appendix)
- Children's work can only be published with the permission of the child or parents/carers.
- When searching for images, video or sound clips, children will be taught about copyright and acknowledging ownership.

Managing ICT systems and access

- The school is responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems is based upon a ‘least privilege’ approach.
- Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software are kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- At Key Stage 2, children will have an individual user account with an appropriate password for their Google Apps account and other online learning zones, for example: Purple Mash, Sumdog, etc which will be kept secure, in line with the children’s Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the school network using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow children to access the network through their id and password. They will abide by the school AUP at all times.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Yorkshire and Humberside Grid for Learning (YHGfL)
- The school's internet provision includes filtering appropriate to the age and maturity of children.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- Staff directly involved in teaching have access to an id and password which provides access to a different level of filtering than the default. This might be used, for example, to access YouTube videos appropriate for learning. Browsers must not be allowed to remember this password. If this has happened inadvertently the password must be removed, by seeking technical support if necessary. Once staff have accessed this filtering level on a device:
    - they will not leave that device without closing all browser windows
    - they will not allow children to use that device.

- If staff directly involved in teaching plan for children to access a website normally blocked by YHGfL then they will use the following procedure:
    - staff will use their access to Swurl filter management system to allow the site to the appropriate group
    - staff will log that change on Springfield's filter report system
    - this reporting system will be regularly monitored by the eSafeguarding Co-ordinator cross referenced with the Swurl groups

- The school has a clearly defined procedure for reporting breaches of filtering. All staff and children will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, and CEOP.
- The school will regularly review the filtering product for its effectiveness.
- The YHGfL system blocks all sites on the Internet Watch Foundation list and this is updated daily.
- children will be taught to assess content as their internet usage skills develop.
- children will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Children’s access to the school network is via class id. This is only to access learning resources not for saving personal learning.
- All Key Stage 2 children have a personal Google Apps for Education id and password. This is used for saving individual children’s work.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and children have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and children will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

- All staff and children will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, including:
  - Do not write down system passwords.
  - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
  - Always use your own personal passwords to access computer based services, never share these with other users.
  - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
  - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user’s files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school’s personal data policy.
- Users should create different passwords for different accounts and applications.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Data Protection

Personal Data

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.

Springfield School Senior Information Risk Owner (SIRO) - Linda Joseph (Acting Headteacher)
Springfield School Senior Information Asset Owner (IAO) - Joanne Hanney (Office Manager)

- At all times take care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used 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 or their computer is locked when left unattended.
- Data is transferred using encryption and secure password protected devices.

■ When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the data must be encrypted and password protected
  - the device must 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 once it has been transferred or its use is complete.

■ The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
■ The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
■ All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
■ Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
■ All access to information systems should be controlled via a suitably complex password.
■ Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
■ All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.

- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and children will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

Email

- Professional email communications between Springfield staff are via professional email accounts (eg springfield.sheffield.sch.uk)
- The names of children or other sensitive information is not included in the body of the email.
- When it is necessary to transfer personal or sensitive date by email it is communicated in an encrypted attachment.

FAX

- The school fax machines is situated within the administrative office which is a controlled area.
- Staff are vigilant to ensure all sensitive information or personal data sent or received by fax remains secure.

Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. Members of the school community need to be clear on the current state of appropriate use:

Mobile phones belonging to school adults:

- should be kept securely out of sight during learning time and at other times in the company of children
- should never contain images of children who are part of the school community unless pre-agreed with the eSafeguarding Co-ordinating (for example, pictures of family members)

Mobile phones belonging to children:

- may be brought to school with prior agreement by a member of the Senior Management Team
- will be given in at the school office on arrival at school and collected on departure

Hand-held devises, eg PDA's tablets, etc belonging to school adults

- may be used in school subject to the other sections of this policy
- will not be used by children
- will not contain personal data of children or other school information of a sensitive nature

Hand-held devises, eg PDA's tablets, etc belonging to children

- may not be brought to school

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

- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / children or parents / carers (email, chat, etc) must be professional in tone and content.

Unsuitable / inappropriate activities

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

The following actions are 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
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK

The following actions are unaccaptable

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:

- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by YHGfL and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

then actions will be taken according to the Response to incidents of concern flow chart (see appendix)

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

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 behaviour / disciplinary procedures.

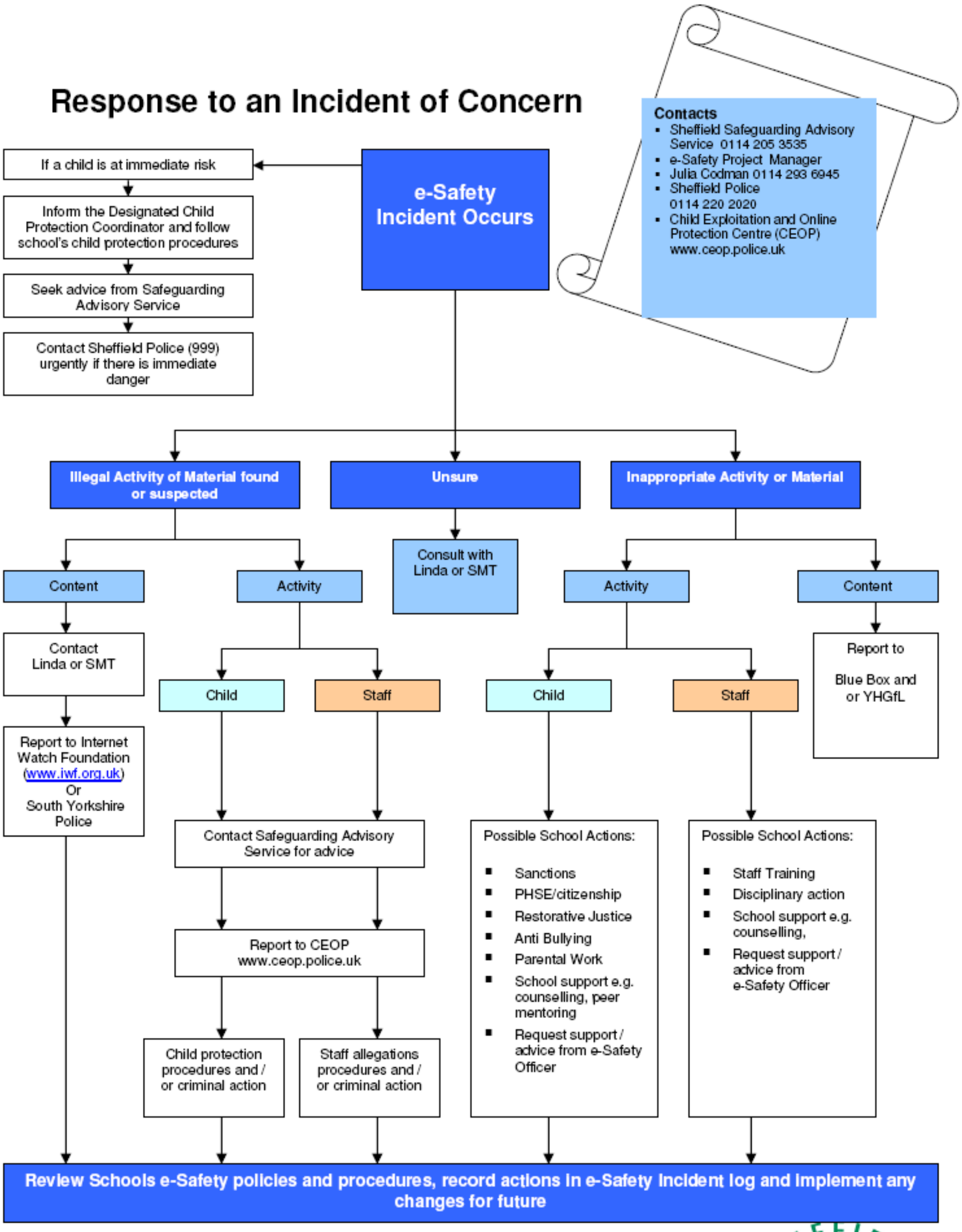
In the case of children such incidents might include:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other handheld device
- Unauthorised use of social networking / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's / pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

In the case of adults such incidents might include:

- Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
- Unauthorised downloading or uploading of files
- 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
- Careless use of personal data eg holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanction

Appendix 1 - Response to an incident of concern



Response to an Incident of Concern

e-Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisory Service

Contact Sheffield Police (999) urgently if there is immediate danger

Contacts

- Sheffield Safeguarding Advisory Service 0114 205 3535
- e-Safety Project Manager
- Julia Codman 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk

Illegal Activity of Material found or suspected

Content

Contact Linda or SMT

Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police

Activity

Child

Staff

Contact Safeguarding Advisory Service for advice

Report to CEOP www.ceop.police.uk

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Unsure

Consult with Linda or SMT

Inappropriate Activity or Material

Activity

Child

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from e-Safety Officer

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from e-Safety Officer

Content

Report to Blue Box and or YHGfL

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future

Contact Details

Schools Designated Child Protection Officer: Hannah Smith/Linda Joseph
School e-Safety Coordinator: Linda Joseph
Safeguarding Children Board e-Safety Manager:

Appendix 2 - Child agreement

Springfield Children
Learning safely through technology.

I understand that I must use school computer and communication systems in a responsible way, to make sure that there is no risk to my safety or to the safety of these systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password with anyone or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology to support our learning:

- I understand that the school ICT systems are for learning and that I will not use them for personal or recreational use unless I have permission to do so. .

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I understand that the school has a responsibility to keep the technology secure and safe:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful

programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed

When using the internet for research for my school work, I understand that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

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

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this is cyberbullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Agreement, it will lead to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student / Pupil Acceptable Use Agreement Form

This form relates to the student / child Acceptable Use Policy (AUP), which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, website etc.

My name ____________________

Class ______________________

Signed Date

Acceptable Use Policy for Young Children (up to and indluding Y3)

This is how we stay safe when we use computers:

I will ask *a teacher / an adult* if I want to use the computer

I will only use activities that *the teacher /an adult* has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from *the teacher / an adult* if I am not sure what to do or if I think I have done something wrong.

I will tell *the teacher / an adult* if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……………………………………………

Signed (parent): ……………………………………………..

Appendix 3 - Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of children, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of children will only be used as stated in the school image use policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School network to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of children within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to a member of the Springfield safeguarding team as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Linda Joseph the e-Safety Coordinator as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to Bluebox support as soon as possible.
- My electronic communications with children, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.
- I will promote e-Safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with Linda Joseph, the e-Safety Coordinatoror, or the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……………………….... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………….