Springmead School

Date: 17/08/2022
Review period: 1 year

Online Safety Policy

This is a whole school policy including EYFS and is audited regularly using 360 Degree Safe

Introduction

This policy should be read alongside the Safeguarding Policy, Computing Policy, Recruitment Policy, Staff Code of Conduct and Handbook, Behaviour and Discipline Policy, Remote Learning Policy and the PSHE Policy. 360 Degree Safe is used to ensure that this policy is kept up to date and that we are following current guidelines.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher, classroom teachers, support staff, parents, volunteers, members of the community and the children themselves.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Susceptibility to radicalization (See risk assessment for Prevent)
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online-bullying
- Access to unsuitable online gaming
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school demonstrates that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Roles and Responsibilities

This policy applies to all members of the school community (including staff, students, children, volunteers, parents / carers, visitors), who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers 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 is pertinent to incidents of online-bullying or other online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online Safety behaviour that take place out of school.
The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

- Technical Support - Nick Munckton / Sally Cox / Geeking it Simple/Frome Tech
- Password issues - Kim Hobley and Sally Cox
- Curriculum – Jemma Stickley and Sally Cox

The Headteacher:

The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, although the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.
The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant
The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
The Headteacher will receive regular monitoring reports from Johanna Robinson/ Carol May/ Shirley Offer.

The Headteacher should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online Safety Coordinator:
Springmead School has a named member of staff with a day to day responsibility for Online Safety. This person is Shirley Offer. The role of the online safety Coordinator:
leads the Online Safety committee
Regularly receives advice from CEOPs and the DSL
takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
provides training and advice for staff
liaises with the Local Authority
liaises with school ICT technical staff
receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments,
reports regularly to the Headteacher and to all other staff.

Supporting Online Safety Coordinator – Johanna Robinson ensures that:
users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed every 90 days. The Class Teacher will also hold a list of passwords securely for Key Stage 1.
the management and monitoring of 'The Smoothwall System'. This system filters and logs the internet content by user. The system has default rules to shield our users from different categories of content. With this system it is possible to create different access levels. E.g. Staff have different levels of access to children.

Technical Support Person (Geeking it Simple/FromeTech):
Geeking it Simple/FromeTech, provides external ICT support for Springmead School.

FromeTech helps us to ensure as best as is reasonably possible, that the school's ICT infrastructure is secure and is not open to misuse or malicious attacks.

The Online Safety Committee ensures:
that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Use agreements with staff, parents, volunteers and children and any relevant Local Authority Online Safety Policy and guidance
that the school keeps up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
that the use of the network /Google Classroom / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator/ Headteacher/ Computing Lead / Class teacher /Support staff for investigation / action / sanction

Subject Leaders
The Computing leader role is to Gemma Stickley

Regularly research advice from CEOPs
Ensure that password changes take place every 90 days for all staff and children
provides training and advice for staff
ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
provides training and advice for staff
liaises with school ICT technical staff
receives reports of Online Safety
reports regularly on Online Safety issues to the Headteacher and to all other staff.

Teaching and Support Staff

They have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices:

- they have read, understood and signed the school staff acceptable use agreements
- they report any suspected misuse or problem to the Online Safety Co-ordinator, Headteacher, ICT Leader/ Class teacher / for investigation / action / sanction
- digital communications with children (email / voice) are on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- Children understand and follow the school Online Safety and acceptable use policy
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead and Deputy

At Springmead School, , Sally Cox is the Designated Safeguarding Lead and and Nick Munckton is the Deputy Designated Safeguarding Leads for the whole school and EYFS They are both trained in Online Safety issues and are aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online bullying

- sexting
- child on child abuse

Working Committee

A working committee consists of all those in the school who have responsibility for Online Safety including:
Madeleine Taylor, Shirley Offer, Johanna Robinson and Sally Cox.

Children
The children at Springmead School :

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use agreement, which they will be expected to sign before being given access to school systems. (At KS1 parents / carers sign on behalf of the children) All children within the school sign an agreement half termly agreeing Acceptable Use which is then displayed in the classroom. Parents sign an Acceptable Use Agreement at the beginning of each school year.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents 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' evenings, newsletters, letters, website / VLE and information about national / local Online Safety campaigns / literature. Parents and carers will be responsible for endorsing (by signature) the Pupil Acceptable Use agreement annually or when necessary. **We regularly highlight online safety issues and publish articles through our newsletter.**

Policy Statements

Education – children
Whilst regulation and technical solutions are very important, their use must be balanced by educating students / children to take a responsible approach. The

education of children in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- We are continuing to develop a planned Online Safety programme which is provided as part of Computing/ ICT / PHSE / other lessons and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school.
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Children are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Children are helped to understand the need to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all rooms.
- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers may have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

Letters, newsletters and website,
Parents evenings
Reference to the SWGfL Safe website
Reference to Thinkuknow website

Education & 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 programme of formal Online Safety training is available to staff.

An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.

- All new staff receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use agreements
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The Online Safety Coordinator/ICT Subject Leader will provide advice / guidance / training as required to individuals as required

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also needs to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities.
School ICT systems are managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage agreement
There are regular reviews and audits of the safety and security of school ICT systems
Servers must be securely located and physical access restricted.
All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be reviewed, at least annually.
All users (at KS2 and above) will be provided with a username and password byGeekingIT. An up to date record of users and their usernames will be kept on theMicrosoft 365. Users will be required to change their password every 90 days.
The "administrator" level passwords for the school ICT system, can be used by FromeTech and Madeleine Taylor and are kept in a secure place. A site documentation is held off site by our ICT Consultants, FromeTech.
Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to Shirley Offer - Online Safety Coordinator.
The school has provided enhanced user-level filtering through the use of the Smoothwall filtering software.
In the event of FromeTech needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
Staff have access to all sites. Their internet access is monitored.
Requests from staff for sites to be removed from the 'student filtering' will be considered by the Online Safety Committee and actioned by FromeTech.
School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this monitoring by screen prompt when logging on.
An appropriate system is in place for users to report any actual / potential Online Safety incident to the Committee. There is a log book available that lists incidents.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. The Guest log is monitored by FromeTech.
An agreed policy is in place (to be described) regarding the downloading of executable files by users
An agreed policy for Holiday club to only use a holiday club log in during opening hours. Children would not use their school log in. The children would have restricted use of sites to ensure online safety during the session. This password would be changed on the last day of holiday club as part of the tidying teams.
Regarding the use of removable media (eg memory sticks, hard drives, CDs , DVDs by users on school workstations / portable devices. These are not recommended as staff have access to Sharepoint to be able to securely access school files and work remotely. Microsoft Sharepoint is a way to securely access documentation remotely, this will be increased over the academic year and memory sticks will be phased out.
Our virtual learning environment is used by staff and children and can be accessed remotely. Children and Parents have signed a remote learning agreement.

Personal mobile telephones, devices, cameras and memory sticks

The following guidelines are designed to protect ourselves as well as the children in our care.

Main School and EYFS Classes (Nursery and Reception)

There have been several high-profile cases of child abuse related to the use of mobile phones. Our need to protect children is paramount as is our need to protect our professional integrity.
This policy provides guidance on the appropriate use of personal mobile phones or personal tablets by members of staff, including the potential consequences of misuse.

- Staff use of mobile phones when with children should be limited to professional use and only used where you are unable to achieve the same results on school technology. For example, taking crisp photos or speedily uploading Google Classroom comments.
- Mobile phones should be stored away from children, preferably not in the classroom, especially the nursery, after school or holiday club.
- Staff must exercise great professional integrity and caution when using mobile phones in front of children.
- Photographs taken must be deleted within 48 hours.
- Personal calls should not be made or taken in the presence of children.
- If a private call needs to be made/received a request should be made to the Senior Management Team.
- Staff should not send or read texts/messages in front of children.
- Staff should never use mobile phones as a form of personal entertainment when with children.
- Staff should never contact children from their personal mobile phone, nor give their mobile phone number to children.
- If a member of staff needs to make telephone contact with a parent, a school telephone should be the preferred option.
- Staff should never send texts or images that could be viewed as inappropriate.

- If an inappropriate text or image is received, this must be reported to the SMT.
- Staff should understand that failure to comply with the policy is likely to result in disciplinary action or even a safeguarding issue and would be dealt with in line with our disciplinary procedures.
- We reserve to right to check mobile phones.

Curriculum

Online Safety is a focus in all areas of the curriculum and staff reinforce Online Safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where children are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that they are temporarily removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Children are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital, online and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / 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 students / 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 e.g. 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 Internet, 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 is obtained before photographs of students / children are published on the Internet. This is in the Terms and Conditions of the school that parents sign on registering their child at the school.
- Zoom sessions have been used during Remote Learning sessions by teachers and children due to Covid-19 restrictions. Parent and Pupil remote learning agreements were signed prior to its use and sessions were recorded for safeguarding reasons.

Staff Use of Internet and Email

- All internet activity should be appropriate to staff professional activity or pupil education.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Access should only be made via the authorised account and password.
- Unsuitable material (pornographic, racist, and offensive) must not be deliberately accessed and downloaded. Should unsuitable material be accidentally accessed an ICT technician and the Headteacher must be immediately informed.
- Employees must not become 'friends' of children on social network sites.
- Users are responsible for their email and must ensure that the content is professional and appropriate. Posting anonymous messages and forwarding chain letters is forbidden.
- Email contacts must not be given without the permission of the person(s) concerned. BCC enables emails to be copied without disclosing the email address.
- The content of email must be strictly for the recipient(s) and a disclaimer used on all emails.

Data Protection

Personal date is defined as data (fact and opinion) that is held on a living individual that can be identified from the date itself. The school processes personal data regarding staff, children and their parents/guardians. This involves obtaining, recording, holding, disclosing, destroying and using data. It is important that all staff are very careful about the content of school information as the Data Protection Act allows individuals to find out what information is held about themselves on computer

and some paper records. The school is a registered data controller on the Data Protection Register. This policy forms part of our induction for new staff.
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.

For further information please see the Data Protection Policy
Responsibilities
The Headteacher is responsible for:
Ensuring that this policy is part of the induction process for all staff
Ensuring that the school is registered under the Data Protection Act
Being a data protection controller to ensure that all personal data is processed in compliance with this policy and the Data Protection Act 1998
Ensuring information with regards to children, parents and staff is not released without the written permission of the person concerned
Ensuring the policies are published on the school website

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

Communications

This is an area of rapidly developing technologies and uses.
A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students / children should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- 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 children or parents / carers (email, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.

Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

- Whole class or group email addresses will be used at EYFS and KS1, while children at KS2 and above will be provided with individual school email addresses for educational use.
- Students / children should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
Springmead 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.

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 ie.

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

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.
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.

Incident reporting
We follow advice from SWGfL.

https://swgfl.org.uk/assets/documents/managing-incidents.pdf

Monitoring and review

This policy is the Headteacher's on going responsibility and its effectiveness will be reviewed annually in consultation with the staff.

Signed Headteacher: Sally Cox

Date: 17/8/2022