Purpose

This Online Safety Policy applies to all members of the school community (including staff, children, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). This policy has been written using the template from the SWGFL.

Any issues or concerns can be reported to the Online safety Co-ordinator or any member of the governing body.

New technologies have become integral to the lives of children and young people in today's society, both within the school and in their lives outside.

This Online safety Policy explains how the school addresses issues relating to technology, as well as wider educational and social benefits in order to help staff, school users, children (their parents and carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use. This applies to all devices used within the school i.e. desktop computers, laptops, ipads, CCTV and mobile phones; or any other devices purchased by the school.

It provides safeguards and rules for acceptable use to guide all users in their online experiences. It ensures adults are clear about procedures for misuse of any technologies both within and beyond the school.

The requirement to ensure that our children 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 the school are bound.

However, the use of these new technologies can put young children 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
- The risk of vulnerable learners being exposed to online risk
- Unauthorised access to / loss of / sharing of personal information
- The risk of children being exposed to the risk of 'commerce'
- The risk of being subject to grooming by those with whom they make contact with on the Internet.
- The sharing / distribution of personal images without an individual's consent or Knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / Internet games
- 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 young children. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of any incidents of inappropriate Online safety behaviour that takes place.

Roles and responsibilities

As carers we need to educate the staff, parents, children and users of the school to ensure that everyone is aware of the benefits and risks that can be experienced through today's technology. To be alert to the vulnerability of children, and how as carers, we can provide control and safeguards for all school users.

Children

- Children will be supervised at all times whilst using technology, and online devices and any games or apps used must be from a pre-approved selection checked and agreed by the headteacher.
- Children's use will be restricted to ensure a balance in educational

medias.

- Online searching and installing/downloading of new programs and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.
- Computer systems have separate logins for when children access them to ensure school network is protected.

Users / Staff

- Users to read, sign and understand the **Acceptable Use Agreement.**
- Users to ensure any passwords relating to school programmes are confidential, and all usernames and passwords are kept secure. Staff will also be advised, that it is good practice to change their passwords on a regular basis.
- The administrator passwords are kept to a limited group, for security.
- Users are responsible for the content of all text, data, audio or images that they place on or send over LCC's email or Internet system. Users may not relinquish responsibility for the content posted or sent on their behalf by other members of staff.
- Users must report any issues they encounter with the systems or the way they are implemented to a senior manager.

Leaders

- Will ensure all servers and systems have appropriate security, which is updated on a regular basis.
- Will ensure all wireless devices are accessible only by secure passwords.
- Will ensure all mobile devices have up to date security installed, and where appropriate restrictions are applied.
- Leaders should ensure that the use of Internet and email supports the school activity for which the staff are responsible in the following ways;
- Ensure that the facilities are used in a way that is appropriate to the school,
- Inform staff of school and policy requirements and the extent to which personal use is permitted.
- To ensure appropriate safety when using technology:

The school will:

- Designate a person to undertake the role of Online safety co-ordinator, who is capable of addressing or acting appropriately with any issues which occur relating to technology. Ensuring that the Online safety co-ordinator:
- Remains up to date with all Online safety matters and guidance issued from the Local authority, or as recommended through such agencies as CEOP (Child Exploitation and Online Protection Centre);
- Is involved with the updating of the Schools Online safety Policy and Acceptable Use Policies;
- Fully aware of any incidents which occur, and the reporting/recording requirements needed; Any incidents will be recorded/reporting via the schools safeguarding/complaints/concerns procedure and the following information will be recorded in regards to Online safety:
- Date of the incident, name of individual(s) involved, device number/location, details of the incident, actions and reasons.
- Delivers training / advice, to staff, children, Governors and any other users, to ensure they are kept aware of updates.
- Ensure a safe and secure broadband from the Local Authority is inclusive of an effective web filter;
- Review all IT systems, including security regularly;
- Have sufficient, up to date virus protection available and in use;
- Ensure that all personal data will be appropriately protected according to the Data Protection Act
- Ensure that every action is taken to safeguard users of all the technology equipment throughout the school.
- Ensure all users receive and sign a copy of the **Acceptable Use Agreement**

Staff will:

- Be aware of their responsibilities as users of the equipment;
- Implement appropriate actions to ensure measures are undertaken, to protect other users;

- Educate children in the acceptable use of the internet – with clear learning objectives outlined;
- Educate children in the use of the internet as an effective learning tool;
- Ensure that if in the event of an incident, the matter is reported to and acted upon by the Online safety co-ordinator;
- Ensure emails are used appropriately as per the schools system, and that any misuse such as the sending of inappropriate emails will result in action by the leadership;
- Ensure children are given guidance on the importance of not giving out any personal details on the internet, which can identify them or their address;
- Report any inappropriate sites which may have been accessed, immediately to the Online safety co-ordinator;

Users must:

- Be informed of the rules of the use of I.T. related equipment within the school;
- Observe all the security rules that apply to the use of all technology about passwords, unattended screens and so on;
- Be aware of the educational value of the correct use of technology;
- Be aware of their responsibility as users of the technology provided;
- Be aware of who to discuss any issues which they are uncomfortable with, relating to their, or others use of the technology.

Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents

- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead/Head Teacher, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the LADO
- where there is no suspected illegal activity, devices may be checked using the following procedures:
- one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the

machine being used for investigation. These may be printed, signed, and attached to the form

- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by LADO
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on either CPOMS or Staff Safe
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *Head and staff for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - local authority/external agencies, as relevant

See Appendix for Flow Chart

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the Fairfield Nursery School. The acceptable use agreements will be communicated/re-enforced through:

- school prospectus
- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- school website
- peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
might be classed as cyber-crime under the Computer Misuse Act (1990)	authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Infringing copyright				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Fairfield Specific

The school team have agreed on the following activities when undertaken for non-educational purposes:	**Staff and other adults**				**Children**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								

Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and parents/carers (e-mail) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by head teacher, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The

DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.
The filtering and monitoring provision is reviewed (at least annually) by the head teacher, the back up DSL and a governor with the involvement of the IT Service Provider. Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- With teachers and key workers, children will be supported to use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is

managed in ways that are consistent with school policy and practice.

- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead/Head Teacher, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. Including:

- physical monitoring (adult supervision with the children)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches by the head
- the head regularly monitors and records the activity of users on the school technical systems

TECHNOLOGY / DEVICES IN USE

School Web Site

Fairfield Nursery School website is managed/hosted by FSE Design. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

- The creation of the school web site will only include contact details for the school, and no details relating to individual children or staff members.
- Photos used within the site will be with the permission of parents / carers, and staff members.
- The Headteacher will have the ultimate responsibility for overseeing the materials used within the school web site.
- Photos of the children placed on the website will not have the child's name linked to it.
- Work produced by the children will only be able to be displayed on the site, following permission from the parents /carers.
- Anyone who has any concerns relating to any of the content on the website must direct them to the Headteacher.

Mobile Phones

- The use of mobile phones is not permitted within the building, by staff, children or any other school users during nursery sessions.
- Should a child have a mobile phone with them, they are required to pass the phone to a member of staff until such times as the session is ended.
- Contractors must be reminded that they must not use mobile phones whilst in the school. If a contractor needs to take a picture of equipment or the premises, they must first discuss this with a member of the senior staff and ensure that no children are in the area before a photo is taken and the image must be purely of the area required.

Smart Watches

- Staff who wear smart watches linked to their phones are not permitted to to use them in the building during nursery sessions

Use of USBs

USBs are not permitted in school

Digital Media (ipads)

- All images taken are considered personal data under the Data Protection Act, and must be treated accordingly. The images may be used purely for purposes agreed within the school, e.g. displays, website, brochures and marketing material and learning journeys. These images must not be used for any purpose, where the parents / carers have not signed the school's agreement.
- Parents are not permitted to take any photos within the school

Storage of Photographs / Videos

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will developmentally appropriate, support the children regarding the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that children are appropriately dressed
- photographs published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy
- children's 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 learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

- Any photographs taken for displays etc, will be saved to a secure drive on the school computer system. These photographs will be saved for a presently undefined time, after which they will be deleted by the key worker or headteacher.
- All photographs are checked from the list of permissions by all staff to ensure no photographs containing images of children, who for whatever reason are unable to be shown, are not used.
- When any photographs are used for advertising / publicity purposes, no child will be identified by their full name.

CCTV Footage

- Footage of children and staff within the rooms, is relayed and saved to computer hard drives within the school.
- None of the cameras in the rooms are positioned in or overlook any sensitive areas, within the school.
- Access to the footage is password protected, and those with access is limited to the ICT technician and Head teacher.
- Footage is held for a period of 6 weeks after which time it is deleted from the system, unless there are any issues around a specific piece

of footage in which case this is preserved for the duration of the query.

- In the event that some footage is needed as part of a query, this footage will be copied and given to the investigating member of staff. The original will then be preserved in an archive area of the server, for a period to be agreed by the Head Teacher. Once the query has been dealt with, the copied version of the footage will be deleted permanently.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with the head teacher who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the head
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in the school safe.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school

systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.

- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Gil Rostron and the IT Company are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the head
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile, for example, schools finance team.

Communication Technology

As new technology is introduced to the school, then this policy will be updated, and all users made aware of all changes.

Email

- All staff have email access, which they are requested to use in a correct and professional manner for both internal and external communication.

- Staff are permitted to access their own personal emails via the internet, but not within their working hours.
- All staff are responsible for the control of their emails, and to delete / save emails as appropriate; considering the fact that storage is not unlimited.
- Staff will be made aware that email communication can be monitored at any time, if it is felt necessary by the senior management.
- Any emails received by staff which is felt to be inappropriate must be reported immediately to the online safety coordinator or the Head Teacher
- Key workers use email to stay in contact with parents. If any emails contain children and family details they are to be deleted accordingly (GDPR).
- Misuse of the email system will be reported to the Head Teacher, who will act in accordance with the School's Disciplinary Procedure.

Remote learning

- Teachers work collaboratively with key workers on remote learning and ensure links are connected to a reputable source and is age appropriate for the children.
- Links on the website are connected and checked that they are reputable
- Remote learning is available by email to the parents of the children to ensure parental links.
- The school uses our You Tube channel for children and families to access a variety of remote learning activities

Social Networks (also see Social Networking Policy)

With the widespread use of the Social Network a wider audience is reached, to enable communication and engagement. However, in doing so this means that we have a duty to consider our responsibilities towards our users and partners. As well as our legal duty to safeguard our children, their families, and school users.

The use of any social networking site within the school, must be carried out

appropriately to maintain the integrity of the school. Social networking applications include, amongst many:

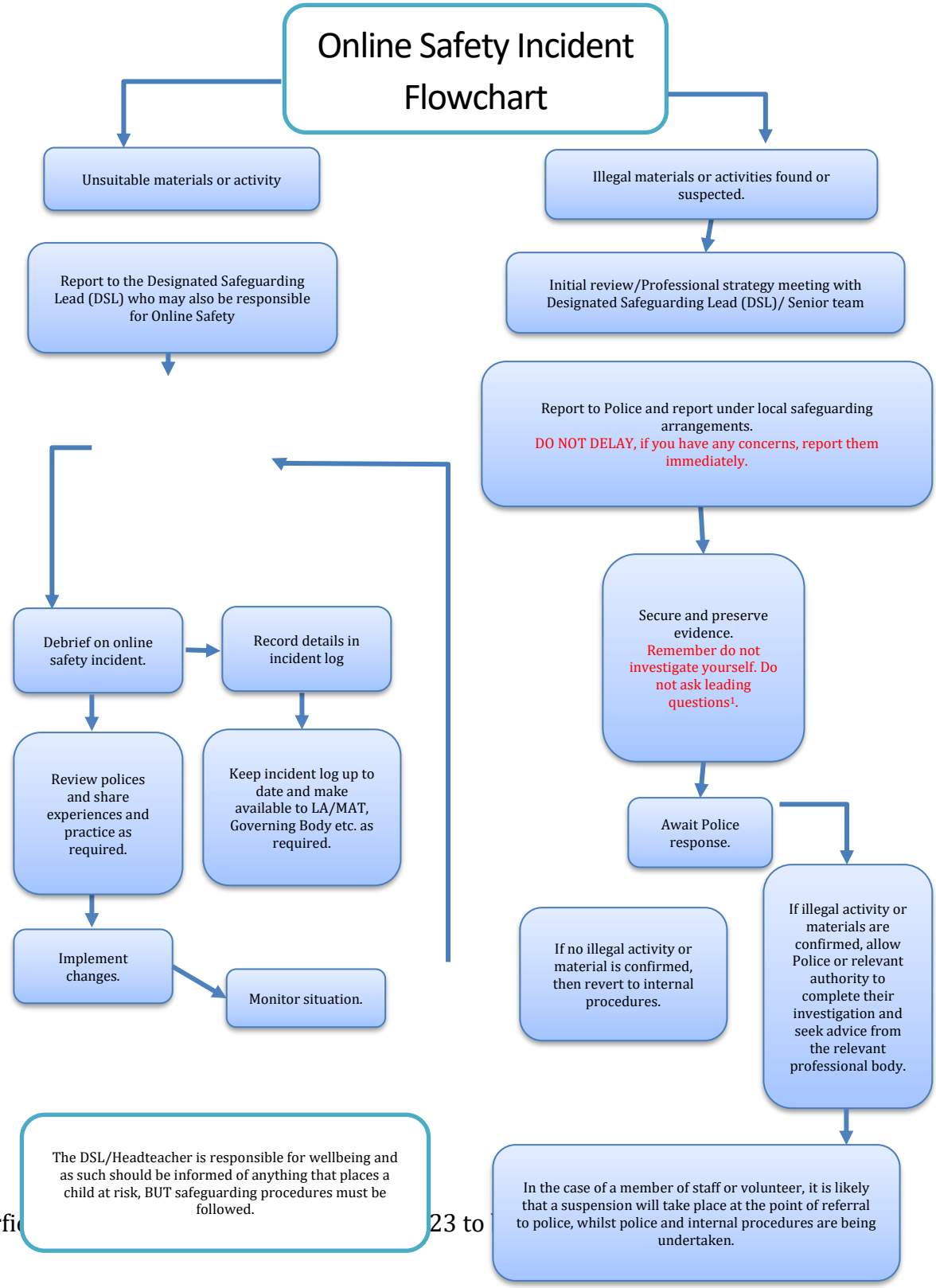
- Blogs
- Forums
- Youtube
- Twitter
- FaceBook

- Children will only be permitted to access social networking sites when working closely with staff, and then only when using it to support learning.
- The school does have its own page on a social networking site, which is used to promote services and events held. This will be controlled by the Headteacher and a limited number of staff. All material posted will be checked by the Head Teacher, and any photos will be checked thoroughly to ensure that they are able to be published. No names of children or staff will be published on the site, and permission will always be gained before any images are used. Checks will be made regularly to ensure that no comments are added to the site, which are inappropriate or offensive to staff at the school.
- Staff must be aware that they must not disclose any information through any social networking site, relating to the school, school staff or users of the school.

DATA PROTECTION

- The Data Protection Act (1998) applies to all materials used and produced throughout the Centre.
- All staff are responsible for ensuring they do not disclose any personal information, and that any personal information they use is not misused or lost.
- Passwords must not be disclosed, and all staff must ensure they log off correctly at the end of a working session.
- GDPR applies to all information given for staff, children and families.

Appendix


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.		x	x	x				
Deliberately accessing or trying to access offensive or pornographic material		x	x	x				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x				
Using proxy sites or other means to subvert the school's filtering system.		x				x		
Unauthorised downloading or uploading of files or file sharing		x			x	x		
Breaching copyright or licensing regulations.		x	x	x	x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		x				x		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		x				x		

Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		x				x		
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		x				x		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		x				x		
Actions which could compromise the staff member's professional standing		x				x		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x				x		
Failing to report incidents whether caused by deliberate or accidental actions		x				x		
Continued infringements of the above, following previous warnings or sanctions.		x	x					x

Appendix

Acceptable Use Policy Agreement – Staff and Volunteers

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement (as taken from SWGFL)

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

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

it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will only use my own mobile device when I am away from children and not in session time. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- 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 not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or child data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....
Signed: .....
Date: .....