



ONLINE & ACCEPTABLE USE POLICY - Federation

Updating Policy Procedure

When a policy is due for review it will be emailed to the reviewer who will revise and highlight those updates and return the policy in full with the highlighted updates back to the Policy Co-Ordinator.

When a policy reviewer becomes aware of any updates they will ask the Policy Co-Ordinator to email the policy to them and follow the above procedures.

A policy is a statement of intent and the guidelines we follow, that is adopted by the Fortuna and Athena Federation's Governing Body.

Policy Reviewed by:

Liam Williams -Fortuna
Paul Swinburne - Athena

Updated on:

Updated January & March 2026

Date to be reviewed:

May 2027

Date Ratified at FGM:

18th May 2026



Online & Acceptable Use Policy

The Fortuna and Athena Federation believes that the use of communication technology and the Internet is an essential and powerful tool for educational, business and social interaction purposes in the modern digital age. As such we will actively promote the safe and responsible use of these technologies, with a view to safeguard and protect all users both within and beyond school hours.

We believe that:

- Online concerns safeguarding children and young people in the digital world.
- Online emphasises learning to understand and use new technologies in a positive and safe way.
- Online is less about restriction and more about educating young people of the risks and benefits of the use of ICT so we can feel safe and confident online.
- Online is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

Aim

As a school we aim to provide pupils and staff with a safe online environment and a curriculum that ensures they become safe and responsible users of mobile and online technologies. This policy will ensure staff are clear of their duties and responsibilities to ensure that this aim can be met.

At the federation there is an effective approach to online safety aimed to protect and educate pupils and staff in their use of technology. There is an interrelated theme linked to safeguarding that runs through all relevant policies and procedures. The federations consider the four areas of risk as outlined fully in paragraph 136 KCSIE of high importance to educating and monitoring children in online safety:

Content: Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).

Commerce: Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If staff feel your pupils, students or staff are at risk, they are to report it to safeguarding leads who will report to the Anti-Phishing Working Group if necessary.

To cover these areas in Fortuna school we have made sure these were embedded into our computing and PSHE curriculum. For both subjects, we have access to 'Kapow'. Even though this scheme does not use the exact terminology, this scheme covers 'content', 'contact' and 'conduct'



through their online safety lessons.

Commerce is covered in the year 5 PSHE curriculum as part of the economic wellbeing strand (year 5- Lesson 4- risks with handling money online).

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective federation approach to online safety empowers, protects, and educates pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Objectives

- To provide pupils with a safe as possible on-line learning environment.
- To identify the risks associated with e-learning environments.
- To identify how e-learning in school will be managed and monitored.
- To identify how the acceptable use of school ICT systems and hardware will be managed and monitored.
- To give clear guidance and procedures to staff and pupils concerning inappropriate material accessed on the web.
- To provide clear guidance to parents about their child's use and access to the Internet and other communication technologies within school.

What can an online policy provide?

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. Internet communication can also provide opportunities for adults to make inappropriate contact with children. The online policy provides clarity on what is permitted and what is inappropriate and aims to safeguard and protect pupils and staff.

Parents and pupils sign an acceptable user policy together when a pupil first starts at the school. The class rules, and the acceptable use agreement, are then signed annually by pupils and shared with parents.

All staff and volunteers with access to Fortuna/Athena Federation ICT systems and hardware must sign and adhere to the online and Acceptable Use Policy (AUP) showing that they accept that the school can monitor network and internet usage to help ensure staff and pupil safety. In doing so, staff are also acknowledging that should they breach the online and AUP they risk facing disciplinary procedures including dismissal.

School Visitors are not permitted to use mobile phones or other equipment (including laptops and tablets with integrated cameras), which have a camera or audio recording function where pupils are present whilst in the school, unless this is pertinent to their visit and the permission of the Head teacher and legal guardian has been provided.

Smart watches with limited capability are acceptable for use in school. Watches that have internet and phone capability are not permitted beyond the staff room.

All smart watches must be in aeroplane mode while outside of the staff room and phone calls, messaging and internet access is not permitted in school.

Failure to follow the policy will be subject to potential disciplinary action.

How do we teach online?

At Fortuna School and Athena School we take our responsibility to educate our pupils about keeping safe in an online world seriously.



At both schools we provide a 'stage appropriate' and progressive online curriculum where pupils can work towards achieving national curriculum objectives, this operates on a two-year cycle. Peer mentoring is encouraged through activities such as promoting online through a variety of methods like developing a school online group or organising a safer internet day or contributing to the online board. Fortuna provides a monthly e-safety newsletter which is uploaded to the school's website by the IT subject leader.

At Athena, we develop our student's awareness of online safety. Through a series of activities and course work, our students gain a greater understanding on how to work and thrive within today's growing online workplace. Including safety measures, etiquette, and ethics. Not only are these present to ensure the curriculum is met within our lessons but there is also a body of students who are E-Safety ambassadors within the year groups.

The E- safety ambassador's roles include being an approachable source for fellow students if they don't feel comfortable talking to an adult. On top of this they are also working on methods to improve the school's e-safety knowledge in a way that is digestible by fellow students. They also take part in parent/carers open events to provide information on keeping students safe online and promoting the use of parental controls and privacy settings. The students also have an e-safety lesson at least once every half term.

School Staff

Internet access – staff must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.

It is recognised that under certain circumstances inadvertent access may happen. Should a member of staff or pupil access any of these sites unintentionally the matter should be reported to the Senior Management Team so that it can be recorded in the online Incident Logbook (kept in CAFO/Assistant Head Office).

Access to any of the following should be reported, by the SMT, to Lincolnshire Police: images of child abuse.

Staff must not use the school Wi-Fi with personal devices.

ARK are currently devising and installing a tracker and filter. Until that is completed, no children are allowed on the internet, unless working directly with an adult.

All internet access at both schools can be tracked through Meraki filter (An MX security device) that will identify the devices accessing the school network and the sites they have visited.

Social Networking – is not permitted by staff in school or using school equipment at home. Members of staff will never knowingly become 'friends' with pupils past or present on any social networking site or engage with pupils with Internet chat in any form, including video, audio or text-based chat. Staff should also fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available. Staff need to check their profiles regularly. Any complaints about staff profiles from parents will be investigated thoroughly, in accordance with LCC guidance.

Use of e-mail - All members of staff should use their professional email address for conducting school business. Use of school email for personal/social use is not allowed. All e-mail content must be transparent and open to scrutiny.



Passwords – Staff should keep passwords private and must not be shared with anyone. Passwords are confidential and individualised to each person. On no account should a member of staff allow a pupil to use a staff login, this is because pupil access is more heavily filtered.

Data Protection – Staff will ensure they keep all information secure by **only** using the school MacBook's or a windows 10 laptop with inbuilt security system. Lost or stolen devices containing school data will be reported to the Data Protection Officer **immediately**. This will be recorded in the Data Protection Breach Incident Logbook (*kept in CAFO Office*).

File Sharing – Technology such as peer to peer (P2P) and bit torrents is not permitted on the Lincolnshire School's Network.

Personal Use – *Staff are not permitted to use school ICT equipment or systems for personal use.*

Images and Videos – Staff and pupils will not upload onto any Internet site images or videos of themselves or other staff or pupils without consent (see Website and Photography Policy).

Use of Personal ICT – Staff must not use their personal ICT equipment where pupils are present. *When on trips or out of school, staff will use their personal mobile phones as agreed by the Head of School prior to the trip.*

Use of Technology by Staff in Classrooms – The federation recognises the significant value that technology holds in the classroom, both in enhancing pupils' learning and experiences and in supporting staff to record and manage key safeguarding and behaviour information. The school also recognises the importance of clear professional boundaries around the use of technology to ensure that staff remain fully present, attentive and responsive to pupils at all times.

Where possible, staff will complete administrative recording tasks, including recording information on CPOMS or Behaviour Smart, away from direct pupil interaction. This should take place at designated areas within the classroom environment, such as a back table or kitchen area. During these times, another member of staff must remain with the pupils to ensure consistent supervision, support and safeguarding.

The completion of administrative tasks during the school day should be directed and facilitated by the class teacher to ensure that pupil supervision and learning are not compromised.

To support safeguarding, professional conduct and high-quality interactions with pupils, staff are discouraged from:

Using a device while they are the sole adult responsible for supervising and supporting pupils.

Taking devices into pupil-focused areas of the classroom, such as carpet areas, gathering areas or sofa spaces.

Using a device to record information while seated beside a pupil or engaged in direct one-to-one interaction.

Failure to adhere to these expectations may be addressed in line with the school's safeguarding and staff conduct procedures.



Safe keeping of IT Equipment



Laptops, Chromebooks and Ipads are stored in a secure room with access only possible via master key held by SLT.

- The equipment will have one person responsible and a deputy in their absence, nobody else will have access to the iPads or laptops unless permission is sought from the responsible person or SLT.
- Each class will have equipment signed out by the designated IT handler on request.
- If a class requires the use of the equipment this must be booked with the responsible staff member in advance and booked back in by 3pm end of day before students vacate the building for safeguarding.
- Ideally equipment should not leave the allocated classes possession, however if this occurs the designated IT handler must be informed to ensure all equipment is trackable and returned accordingly.



New I Pads are kept in a lockable charging unit the store cupboard. Each class is assigned a day to use, one member of staff from each class is assigned to remove and put back units. When placed back the I pads and computers must be plugged in. All units must be signed out and in.

Some children are given an amazon fire tablet for their long journeys. This is kept in the class during the day and either in the taxi or the children's house overnight.

The loss or theft of a computer, tablet, data drive or any other device that contains personal data of staff or children should be reported **immediately** to the Data Protection Officer.

Viruses and other malware – Any virus outbreaks are to be reported to the ICT Coordinator or Online officer, as soon as it is practical to do so, along with the name of the virus (if known) and actions taken. Suspicious or unknown emails or links should not be opened.



Using the Internet to support learning (pupils)

Staff and children have Internet access, which has firewall security and age-appropriate filtering through a hardwired system.

Most Internet use is safe, purposeful and beneficial to the pupils, however there is always an element of risk. Within The Fortuna and Athena Federation the greatest risk is through inadvertent access. The school is connected to the Internet through a broadband connection, which means that inappropriate images can appear almost instantaneously from a perfectly appropriate keyword search. Children can also innocently follow a series of links to undesirable content.

Filtering and Monitoring Securely System (Securely Filtering) can be used to track access from specific devices at both schools, hence the requirement that pupils access specific, designated devices.

The following procedure is in place for staff to follow on how to handle the situation immediately:

1. Close or minimise the screen immediately (DON'T try to navigate away). If necessary, end the task for the rest of the group to prevent further access by other pupils.
2. If pupils saw the page; talk to them about it and reassure them.
3. Later investigate the history of the visited sites to get details to report to the ICT coordinator
4. ICT coordinator or member of the senior management team to report inappropriate site to the online Officer.
5. All incidents to be recorded in the online Logbook.

All children will be supervised at all times, including computing enrichment and any after school / extra-curricular activities, when using the internet (*supervised means all children around the table and staff moving around the seating actively monitoring usage*). Children are allowed supervised access to devices for non-educational leisurely uses during the school day, to allow the promotion of computer literacy driven by the learners own motivations.

Where possible teachers will have carried out a subject based search prior to the lesson to ensure that inappropriate material is not accessed. Good planning and preparation are critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an internet-wide search engine, however ARK smartpac is in place to ensure such terms are blocked.

The CIPA guidelines require schools to block students' access to "inappropriate matter on the internet," which includes obscene and pornographic content. securely Filter helps to ensure that all such content is blocked.

To ensure that kids are protected from all forms of inappropriate and malicious content on the internet, we have segmented our database into a range of categories, including Pornography, Drugs, Gambling, Social Media, Hate, Games, Social Networking, etc. (*These categories are listed under 'Blocked Categories' in your 'Policy Editor'.*)

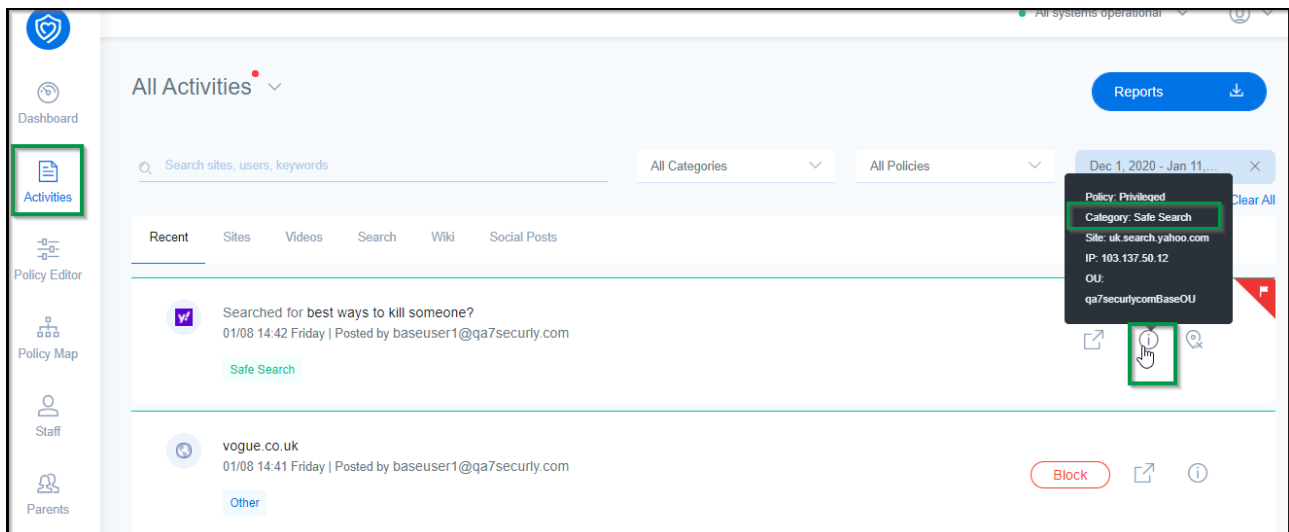
Any new website that does not exist in the database is marked as "Uncategorized" and blocked if the admin has configured it to be blocked. Our PageScan tool automatically scans it when a user visits it for the first time and is categorized appropriately. This is available for both securely extension and SmartPac users.

You can find out why a particular site was blocked by looking at the user activity in securely Filter. To do this:

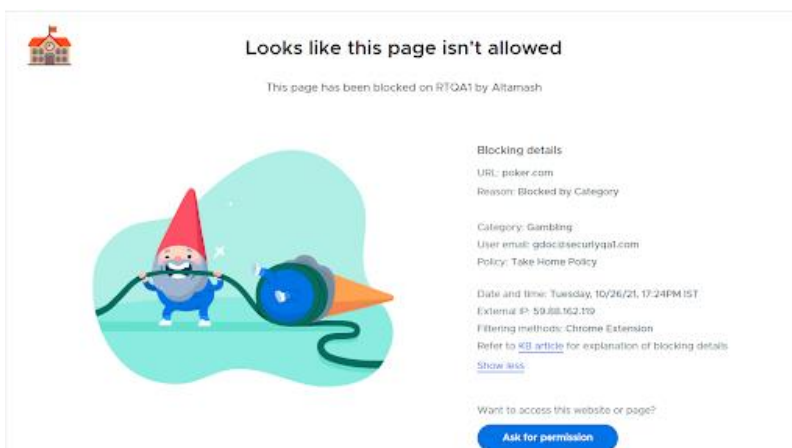
1. Log in to securely Filter and navigate to the Activities page.



- Click the 'info' icon for a blocked event to view details of what category the site belongs to and the policy it was blocked under.



You can also determine why a site was blocked by looking at the blocked page on the user's machine.



It is strongly recommended to staff that videos from streaming websites with advertisements, such as YouTube, are downloaded prior to their use. These should be watched in full to ensure that the content and level are appropriate. The ICT coordinator can support staff who are unsure how to do this.

All children will be aware of the rules of using the Internet in school. Teachers/staff will continually remind children of these rules. Online sessions will be planned for and taught regularly as part of the wider school curriculum and key points pertinent to a learning activity should be recapped before children begin a task. Pupils will be taught which Internet use is acceptable, which is not and given clear objectives for safe and responsible Internet use.

The use of the Internet is accepted as a valuable resource to a child's education and learning. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet in education. Fortuna and Athena see the following benefits of using the Internet in education:



- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- exchange of curriculum and administration data with the LA and DfES;
- access to learning wherever and whenever convenient.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.



Logins and Passwords –

At Fortuna the children use a shared login with adult supervision so that usage can be tracked. The children have access to a 365 account. The computing lead has all children's log in and passwords. Childrens work on the iPad can be saved on the cloud for them to access. Children are taught the importance of logging out through the curriculum. Staff each have an individual login with associated permissions relevant to their role. Staff login details should not be shared.



At Athena every person has a different computer login. Pupils should never allow anyone else to use their details. Staff each have an individual login with associated permissions relevant to their role. Staff login details should not be shared. Class teachers have access to class pupils' passwords and students have personal cloud storage to collate their work.

Mobile Phones – Children will not bring mobile phones or gaming equipment, into school or into the school taxis - at Athena, pupils can bring their mobile phones/tablets but are not allowed to access them during the school day and they are locked away in a secure box within the classroom. When a child's individual circumstance makes this unavoidable (e.g. shared custody or respite care) a procedure will be agreed between home and school at the discretion of a member of the Senior Management Team.

Staff will not keep their mobile phone on their person during the school day. The mobile phones will be kept with their personal belongings in the staff room and only accessed during non-contact time during breaks. If staff are waiting for an urgent call the school number can be given and the member of staff informed by the admin team. In mitigating circumstances staff are to discuss a plan with the Head of School.

The Education Act 2011 provides teachers with the powers to search pupils and their property for mobile devices if it is believed it has been used for an offence (such as images of child abuse or cyber-bullying). The legislation also allows teachers to search for and confiscate a mobile device brought into school if they have been banned by school rules and identified as an item that may be searched for in the school written school rules.

Devices can be confiscated as the result of a search. Any device considered detrimental to school discipline may also be confiscated, regardless of how it was discovered.



Under Article 8 of the European Convention of Human Rights pupils have a right to expect a reasonable level of personal privacy and such searches should be justified and proportionate.

The decision to search a pupil or confiscate an item must be made by the Head of School. It should be carried out by a member of the same sex, witnessed by another member of staff and only done as a last resort.

DVDs/Games

In school, children will only view films or games of an age appropriate level ('U' only for films and 'PEGI 7' for KS2 'PEGI 3' for KS1 or below for games). For PG certified content a signed consent letter from parents will be needed. At Athena, KS3 and KS4 sometimes access Age 12 DVDs, providing all the pupils are 12 and above - some year 7 classes cannot, therefore, access these. However, staff should not take an age rating as a guarantee that a film is appropriate for a class and it should be vetted before being shown to their students. Websites such as Common Sense Media can also be used to check the content of any films.

Social Networking and Online Gaming, Streamed, Terrestrial or DVD Blu-ray Movies or TV Shows.

Although we do not allow social networking, online gaming or the viewing of non-age-appropriate media at school, we are aware that pupils may have access to such at home. Children are taught and regularly reminded about the risks of these activities and how to safeguard themselves online.

If staff are aware of children accessing social media or games, movies and tv shows which are aimed at an older audience a CPOM's form must be completed in-line with school safeguarding procedures.

Use of School-Issued Tablets During Taxi Transport.

Pupils at Fortuna School who experience extended travel times or difficulties with transitions may be provided with a school-issued Amazon Fire Tablet to support their journey to and from school. All devices must be brought into school at the start of each day and returned home with the pupil at the end of the day. The tablet may remain in the taxi or be taken into the home environment, as appropriate.

The Technology Lead Teaching Assistant is authorised to monitor and review all online activity conducted on these devices to ensure safe and appropriate use. Each tablet is preloaded with approved applications and games; pupils must not download or install any additional content independently. If a pupil wishes to request additional applications, they must first consult their class teacher. The request will then be referred to the Technology Lead, who will assess and determine whether the application is suitable and appropriate for use.

Access to Wi-Fi is restricted and secured via password protection.

Can we make a plan to deal with online communication out of school – Whilst online gaming is used outside of school, we understand that pupils may communicate via these platforms. As responsible users of the Internet, all pupils, whether at school or at home, should adhere to the Acceptable Use Agreement.

If staff are aware of children accessing social media aimed at an older audience a concern form must be completed in-line with school safeguarding procedures.



Email



Children use email at Fortuna, and this is introduced as part of the computing curriculum in Stage 2 (Using Ollk – a system that provides school with the ability to physically filter and preview emails before children receive them). All children will be supervised at all times when using email and will not be permitted to submit emails to addresses unauthorised by their class teacher.

The following statements of use reflect Fortuna's policy on the use of e-mail:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.



At Athena the children each have an email account. This Should only be used under the supervision of the class teacher and for the appropriate reasons.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.

Staff and pupils need to understand that the use of the school's network is a privilege which can be removed should reason arise. All users are expected to adhere to the generally accepted rules of network etiquette. These include:

• Be polite. • Use appropriate language. • Do not get abusive in your messages to others. • Do not reveal the personal address, phone number or other personal details of other users. • Do not use the network in such a way that would disrupt the use of the network by other users.	• Illegal activities are strictly forbidden. • Note that e-mail is not guaranteed to be private. • System administrators have access to all mail. • Messages relating to or in support of illegal activities may be reported to the authorities.
---	---

Photographs and video

As part of the curriculum children will have access to digital photography and video. The use of this equipment will be supervised at all times and will only be used as part of planned lessons by the class teacher.

At interview parents/carers can consent for their child and children's work to be photographed and filmed as part of the school's policy for celebrating achievements and children's work this includes permission for children's photographs, video footage, audio extracts and work to be used by school for training purposes.

How should personal data be protected?



The Fortuna and Athena Federation will ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) and other related legislation. It will apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall attend regular training to ensure compliance with their responsibilities

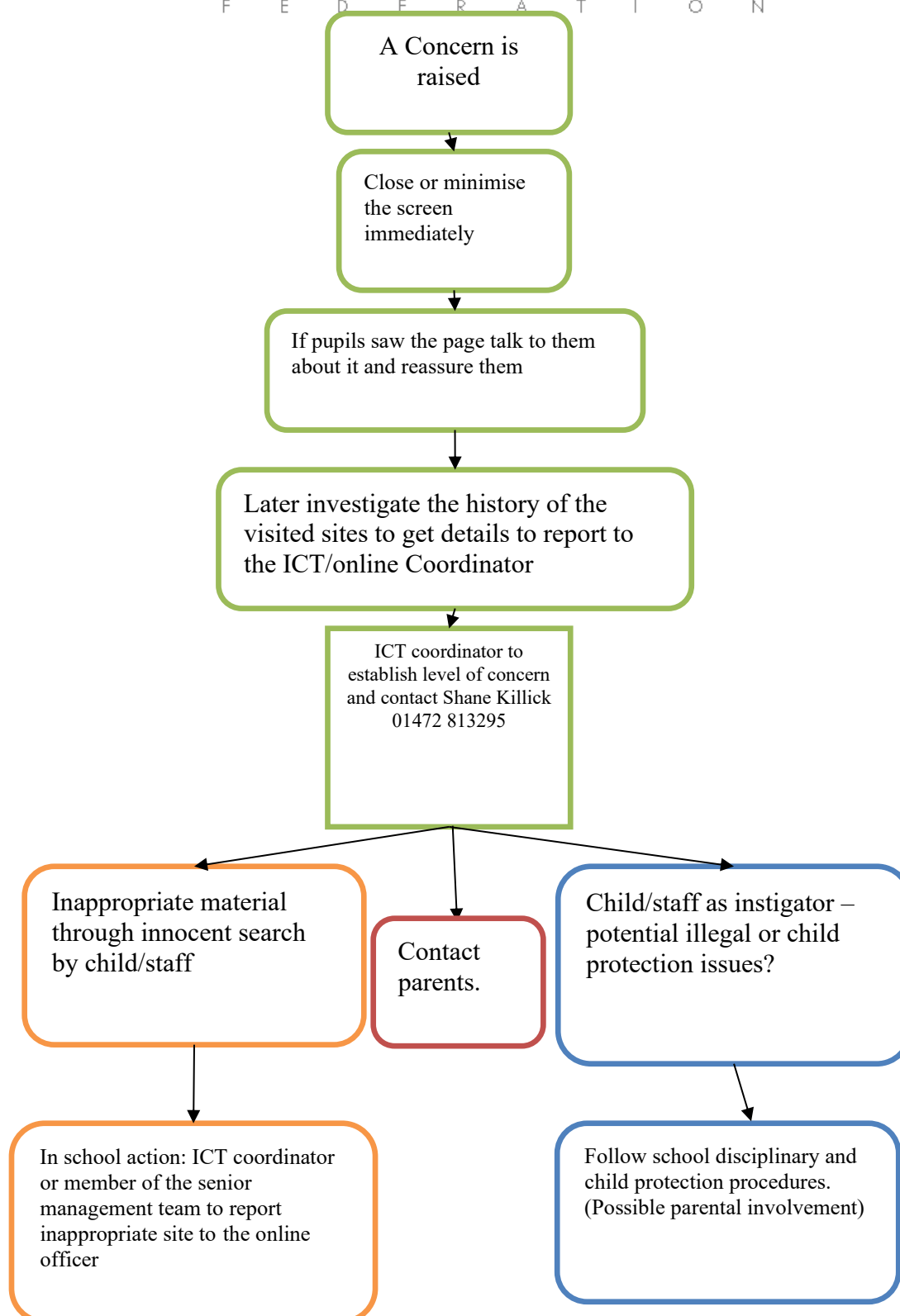
See the Data Protection Policy for full details.

Response to an incident of concern

Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

The Fortuna & Athena Federation will work in partnership with parents; the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address), time, date and content will be reported to the Internet Service Provider, ICT coordinator or Online officer and logged.

The following procedures will be followed in reporting incidents of concern:





What are the risks?

- | | |
|--|---|
| <ul style="list-style-type: none"> ● Receiving inappropriate content ● Predation and grooming ● Requests for personal information ● Viewing 'incitement' sites ● Cyber bullying and threats ● Identity theft | <ul style="list-style-type: none"> ● Publishing inappropriate content ● Online gambling ● Misuse of computer systems ● Publishing personal information/ images ● Hacking and security breaches ● Radicalisation |
|--|---|

How will online complaints be handled?

Parents, teachers and pupils will know how and where to submit a complaint as per school policy, by reporting any concern to the class teacher, in the first instance. Prompt action will be taken if a complaint is made. The facts of the case will be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by a senior member of staff or the Head of School. Complaints of a child protection nature will be dealt with in accordance with school child protection procedures. Potential illegal use will be discussed with the police.

- Complaints of Internet misuse will be dealt with by SMT.
- Any complaint about staff misuse must be referred to the Head of School.

PLEASE NOTE THAT INTERNET AND EMAIL MAY BE SUBJECT TO MONITORING

Bridging the gap between school and home.

As from December 2015 all parents will sign a consent form (see Appendix 3)

Age-inappropriate access - If a pupil divulges watching or playing age inappropriate films or games or has access to age restricted social networking sites; staff must log this on **CPOMS** and follow procedure see Appendix 3.

Sexting and SGII (Self-Generated Indecent Images) – Any disclosures of this nature must be logged on **CPOMS** and brought to the attention of SMT immediately.

Cyberbullying – This will be dealt with through the existing anti-bullying policy and logged. It should be noted that Head teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site (Education and Inspections Act 2006).

Monitoring and Reviewing

- Policy reviewed annually
- Incident log for recording incidents and concerns
- Pupil/parent views sort
- Staff audit
- Regular staff training and updates
- Pupil progression through 'e-sense' awards
- All staff, volunteers and governors sign an Acceptable Use Agreement annually (see Appendix 1)

Online Officer

The Online Officer at Fortuna School is Maddison Knights and at Athena School is Debra Houlton. While it is recognised that all staff have a responsibility for online in school, we understand the



importance of having a named person to oversee the risks and issues surrounding the safe use of technology and to cascade this understanding to all members of staff, governors and the children.

Writing and reviewing the online and Acceptable Use Policy

The online Policy is part of the ICT Policy. It has been written following government guidance, LCC guidance <https://www.lincolnshire.gov.uk/lscb> for online safety updates.

Appendix 1

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I understand that I am personally responsible for all confidential data taken by myself from school and will follow ALL the policy procedures.
- If any device or hard copy with confidential information or pictures/movies pertaining to school and individuals therein is lost, stolen or mislaid it must be reported immediately to a member of senior management, management will then contact the relevant authorities for investigation.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with school policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials or filtering breach online Officer (Craig Chaplin)
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *staff-only drive within school* with consent from parents/carers.
- I will follow the school's policy on use of mobile phones at school.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role. I will not knowingly communicate with, follow or become friends with pupils past or present on any social networking site.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use".



- I will ensure all school devices and technology are left securely and locked away.
- I will ensure any confidential data that I wish to transport from one location to another is protected using the school MacBook's or a window 10 laptop with inbuilt security and that I follow school data security protocols when using any such data at any location.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head / Safeguarding Lead* on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will ensure that any work undertaken at home for the Fortuna and Athena Federation is protected by using the school MacBook's or a window 10 laptop with inbuilt security only.
- I understand that the caretaker will have his work mobile on him during work hours in school; however this must only be used in the designated places.

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others online and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature

Date

Full Name

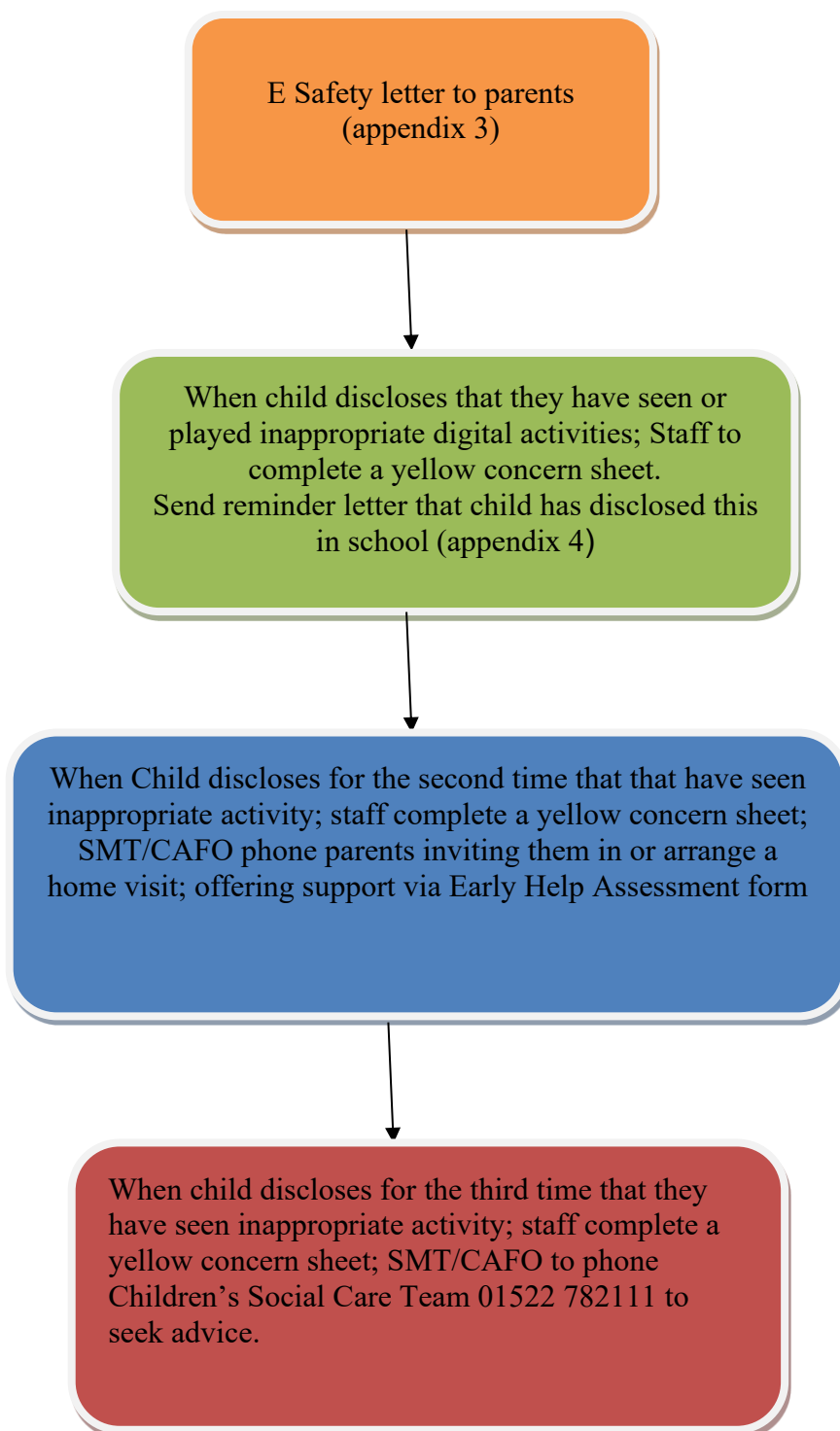
(printed)

Job title / Role



Appendix 2

Online in School and at Home Procedure





Appendix 3

Dear Parents/Carers,

In light of recent concerns that have been raised about children accessing age restricted media, I am writing to all parents and carers to remind you of our statutory duty to safeguard children from inappropriate digital and online content.

As you are more than likely aware all film releases come with a BBFC rating (BBFC.co.uk), or when on television appear before or after the watershed time of 9pm. Content rated U, PG and 12A as well as content broadcast before the watershed are generally considered suitable viewing for primary school aged children, though personal judgement may still be required. Content rated 12 or over may contain varying levels of swearing, physical violence, psychological threat and sexual behaviour.

For computer games PEGI ratings (PEGI.info), a similar classification system to film ratings, are used. Primary aged children should only have access to games rated PEGI 3 or PEGI 7 (depending on their age) to avoid access to inappropriate content.

It is also worth noting that children should not have access to Facebook accounts or webpages, media and messaging sites that are not designed for their age. YouTube can also have inappropriate clips for children.

These are the current age restrictions for social networking sites and accounts.

Facebook, Snapchat, Twitter, Instagram, Musical.ly and Skype require users to be at least 13 years of age. Users of WhatsApp should be at least 16 years of age. While there are no age restrictions on watching videos on YouTube, users need to be 13 years of age or older to have their own YouTube account.

When it becomes apparent that a pupil has viewed media that is age inappropriate content this information will be recorded in the school online logbook and school will contact home to raise any specific concerns and offer support should this be required.

Should it be clear that a child is **consistently** accessing age inappropriate media or has repeatedly accessed media clearly aimed at a mature audience; the school may pass this information onto Children's Social Care Team.

We do recognise that the vast majority of parents and carers are aware of their parental responsibility, but in an ever-evolving digital world the line between what is and is not appropriate can become blurred. If you would like to talk about your child's online or digital safety, please feel free to contact the school and we will do our best to support you.

Please contact us if you require any support in ensuring your child does not access age restricted media.

Yours Sincerely

Hannah Keegan
Head of School



Appendix 4

Dear Parent/Carers

It has come to our attention that your child has repeatedly been accessing age restricted media. He/she has stated that they have been watching/playing I am writing to you, to remind you of our statutory duty to safeguard children from inappropriate digital and online content.

Please contact me if you would like some support regarding this.

Yours Sincerely