ICT & ONLINE SAFETY POLICY

Last Reviewed: June 2023

Document Control			
Review period	24 Months	Next review	May 2025
Owner	CEO	Approver	Audit & Risk Committee

This document applies to all schools and operations of the Galileo Multi Academy Trust:
www.galileotrust.co.uk

Date of changes:	May 2023

Page/ Section	Changes to note	Reason for change *e.g. change in legislation*
	Keeping Children Safe in Education Policy has been updated and version 2022 replaces 2019. The updates to the Online Safety Section of the KCSIE policy were already covered in our policy so no further changes required.	Change in Legislation
Date of final approval:		

Document Control

Monitoring and Review

The implementation of the policy will be monitored by	CEO, CFO, Headteachers & External IT Support
Monitoring will take place using logs of reported incidents, pupil questionnaires and internal monitoring data of network activity	Annually
The online safety policy will be reviewed biennially or if the need arises due to significant changes to technology, new threats or serious incident taking place. The next review will be annually	Biennially
A serious online safety issue should be reported to one of the following	
Designated Safeguarding Lead Deputy Safeguarding Leads Police – 01642 326326 Redcar & Cleveland LADO Lorraine Press Seafield House, Kirkleatham Street, Redcar and Cleveland, TS10 1SP 01642 771530 Independant_review@redcar-cleveland.gcsx.gov.uk	Redcar & Cleveland Local Authority Designated Officer (LADO) 01642 130700 RedcarLADO@redcar-cleveland.gov.uk Redcar & Cleveland Multi Agency Children's Hub (MACH) 01642 130 700 RedcarMACH@redcar-cleveland.gov.uk

Scope of the policy

- This policy applies to all members of Galileo Multi Academy Trust schools, including staff, pupils, volunteers and visitors who have access and are users of school ICT systems both in and out of school
- The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable to regulate the behaviour of pupils 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 cyber-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 Education Act of 2011 increased these powers with regard to searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered in the published Behaviour Policy
- The schools will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform relevant parties of incidents of inappropriate online behaviour that take place out of school.
- Schools in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering "(revised prevent Duty Guidance for England and Wales)
- The DfE published revised guidance for "Keeping Children Safe in Education" in 2022 for school and colleges in England. Included in the revisions, schools are obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or college IT system". However, schools will need to "be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding".

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Galileo schools.

Governors

The Trust's Audit & Risk Committee is responsible for the approval of the ICT & Online Safety Policy and for reviewing the effectiveness of the policy. The Local School Boards (LSBs) of each school will receive regular information about online safety incidents and monitoring reports. A member of the LSB from each school must take on the role of Online Safety Governor. The role of the Online Safety Governors will include:

- Meeting with the Designated Safeguarding Lead at least annually
- Regular monitoring of online safety incidents logs at least annually
- Regular monitoring of filtering
- Reporting to relevant Governor's meeting

Headteacher and members of SLT

- The Headteacher has a duty of care for ensuring the safety including online safety of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead and the Galileo Executive Team.
- The Headteacher and the SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made (Section 4, flow chart page 18).
- The Headteacher and SLT are responsible for ensuring relevant staff receive sufficient training to enable them to carry out other roles.

Headteacher or delegated person

The Headteacher will:

- Take day to day responsibilities for online safety issues and has a lead role in establishing and reviewing the school online safety procedures.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide advice and training for staff
- Liaise with school technical staff
- Compile reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Share the report with the Governing body and SLT

Galileo Executive Team

The Executive Team and technical support staff (including external stakeholders) are responsible for ensuring:

- That the school's technical infrastructure is, as far as possible, secure and not open to misuse or malicious attack
- That the school meet required online safety technical requirements and any academy guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that the implementation is not the sole responsibility of any single person
- That they keep 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, internet, remote access, e mail is regularly monitored in order that any misuse or attempted misuse can be reported to relevant people for investigation

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current trust ICT & Online Safety Policy
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher, SLT or Designated Safeguarding Lead for investigation
- All digital communications with pupils and parents/carers 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 activities
- Pupils understand and follow the ICT & Online Safety Policy and acceptable use polices
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the set of digital technologies and digital devices in lessons and other school activities (where allowed) and implement current policies with regard to these devices

Designated Safeguarding Lead

- Training has been received on online safety issues from CEOP and regular updated training from safeguarding forums.

- The Designated Safeguarding Lead should be aware of the potential for serious child protection and safeguarding issues to arise from:
- Sharing personal data
- Access to illegal and inappropriate materials
- Inappropriate online contact with adults and strangers
- Potential or actual incidents of grooming
- Online-bullying

Pupils

- Are responsible for using the school's digital technology systems in accordance with the
- Pupil Acceptable Use agreement
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and cyber bullying
- Should understand the importance of adopting good online safety practise when using digital technologies out of school and realise that the trust's ICT & Online Safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring their children understand the need to use the internet and digital devices in an appropriate way. The school will help parents understand these issues through newsletters, website and information about both local and national online safety campaigns. Parents/carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video imagery taken at school events
- Their children's personal devices in the school

Policy Statements

Education

<u>Pupils</u>

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risk and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad and relevant and provide progression with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of IT and PSHE lessons and should regularly be revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and PSHE activities
- Pupils should be taught in all lessons to be critically aware of the content they access on- line and be guided to validate the accuracy of the information
- Pupils should be taught to acknowledge the source of information used and to respect

copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making. (The Counter Terrorism Act 2015 requires schools to ensure that children are safe from terrorist and extremist material on the internet)
- Pupils should be helped to understand the need for a Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- It is accepted that from time to time, for good educational reasons, students may need to research topics such as racism, drugs, conflict, discrimination, that would normally be blocked. In such a situation, staff can request that technical staff temporarily remove these sites from the filtered list for the period of study. There must be a record with clear reason for need.

Parents/carers

Many parents and carers 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 and regulation of their children's online behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure how to respond.

Galileo schools will therefore seek to provide information and awareness to parents and carers through:

- Letters and newsletter
- School website information and links to various sources of advice e.g. Child Exploitation and Online Protection Command (CEOP)
- High profile events such as Safer internet Day
- Online reporting of online safety incidents to CEOP https://www.ceop.police.uk/safety-centre/should-i-make-a-report-to-ceop-yp/

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 will be made available to staff. This is regularly updated and reinforced. An audit of online safety training will be carried out regularly
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the trust's ICT & Online Safety Policy and Acceptable Use Agreements
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This ICT & Online Safety Policy and its updates will be presented to and discussed by staff at relevant meetings.
- The Online Safety Coordinator will provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in online safety training and awareness sessions with particular importance for those involved in online safety and safeguarding. This may be offered in several ways:

- Attendance at training provided by the LA/National Governors Association/ or other relevant

organisation
- Participation in school training events

Technical

Infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within the policy are implemented. It will also need to ensure the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets the recommended technical requirements
- There will be regular reviews and audits of the safety and security of the school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by a member of the IT support team. Users will be responsible for the security of their username and password and will be required to change their password at regular intervals.
- The administrator passwords for the school ICT system used by the network manager must be available to the Headteacher or other nominated senior leader and kept in a secure place such as the school safe
- The Trust's external IT Support is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users; illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. The 'police assessed list of unlawful terrorist content produced on behalf of the home office' is integrated. Content lists are regular updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes,
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- Any content listed as a safeguarding concern is logged and emailed daily to the trust's IT support provider. Instant email alerts are configured for suicide. The alerts are checked by technical staff to remove false positives and any remaining alerts that are a cause for concern are forwarded to the school's Headteacher or other designated individual.
- Staff may also monitor and record the activity of users on the school systems using remote management software and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, works stations etc. 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 virus software
- An agreed policy is in place for the provision of temporary access of 'guests' (e.g., student teachers, supply teachers) onto school systems.

Mobile Technologies

Mobile technology devices may be school owned or provided or personally owned and might include smartphones, tablet, notebook, laptop or other technology that has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school allows:

	School Devices			**Personal Devices**		
	School owned devices for single user	School owned devices for multiple users	Authorised devices (such as laptop bought for CIOC)	Student owned	Staff owned	Visitor owned
Allowed in school	YES	YES	YES	FOR EMERGENCY USE ONLY (to be stored in school office)	YES	YES
Full network access	YES	YES	YES			
Internet only					YES	YES
No network access						

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term. It is common for employers to carry 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 pupils about the risk associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks with publishing their own images on the internet.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media or the press.

- 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 is not covered by the EU General Data Protection Regulation). To respect everyone's privacy and in some cases protection these images should not be made publicly available on social networking site, nor should parents/carers comment on any activities involving other students in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of these images. These images should only be taken on school equipment, the personal equipment should not be used for such purposes
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils full names will not be used anywhere on a website or blog particularly in association with photographs
- Pupil's work can only be published but the student should not be able to be identified from the published content

Data protection

Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulations (EU GDPR) which states that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject collected for specified, explicit and legitimate purposes adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed accurate and, where necessary, kept up to date kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed in a manner that ensures appropriate security of the personal data

Every Galileo school must ensure that:

- It holds the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for.
- Every effort is made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the 'Privacy Notice' and
- Lawfully processed in accordance with the 'Conditions for Processing'.
- It adheres to the Trust's Data Protection Policy
- It is registered as a Data Controller for the purposes of the EU GDPR
- Data Protection Impact Assessments (DPIAs) are carried out for all new processing of personal data
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects' privacy rights and there are clear procedures for these to be exercised
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from data breaches and

security incidents
- There are EU GDPR compliant contracts in place with all third party processors
- There are clear policies about the use of cloud storage which ensure that such data transfers and storage meets the adequacy arrangements laid down by the EU GDPR Staff should 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 sessions in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with the school policy once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school considers the benefit of using these technologies for education outweighs the risk

Communication Technologies	Staff and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile Phone may brought to school	X					X		
Use of mobile phone in lessons				X				X
Use of mobile phone in social time		X						X
Taking photos on mobile phones				X				X
Use of other mobile devices e.g. tablets, gaming devices		X						X
Use of personal e mail addresses in school on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs		X						X

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

- The official school email services may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- Users must immediately report, to the nominated person (designated safeguarding leads or deputy safeguarding leads), the receipt of any communication which makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

- Any digital communication between staff and pupils or parents/carers (emails, social media chat, blogs etc.) must be professional in tone and content. These communications may only take place using the official school systems. Personal email addresses must not be used
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
- School email services are provided solely for using for school business and should not be used for personal correspondence

Social Media

<u>Protecting Professional Identity</u>

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies and Local Authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, academies and LAs could be held responsible, indirectly for acts of their employee in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school, academy or LA liable to the injured party. Reasonable steps to prevent harm must be in place.

Galileo schools provide the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through:

- Ensuring personal data is not published
- Training is provided including acceptable use, social media risks, checking of settings, data protection, reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment including legal risk

Galileo staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to schools
- Security settings on personal social media profiles are regularly checked to minimise the loss of personal data

When official social media accounts are established by the school there should be:

- A process approved by senior leaders
- Clear processes for the administration and monitoring of these accounts-involving at least two members of staff
- A code of behaviour for users of the accounts including
- Systems for reporting and dealing with abuse and misuses
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Accounts

- Personal communications are those made via a personal email/social media accounts. In all cases, where a personal account is used which associates itself with Galileo schools or impacts on Galileo schools, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon schools are outside the scope of this policy
- Where excessive personal use of social media in school is suspected and considered to be interfering with relevant duties, disciplinary action may be taken.
-

Monitoring of Public social media

- As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school.
- Schools should effectively respond to social media comments made by others according to a defined policy or process.

The school's use of social media for professional purposes will be checked regularly by the senior leadership team and IT support staff to ensure compliance with the school policies.

Unsuitable/inappropriate activities

Some internet activity e.g., accessing indecent images of children or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g., cyberbullying 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 age of the users or the nature of those activities.

Vision 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 or outside schools when using school equipment or systems. Our policy restricts usage as follows:

USER ACTIONS		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make posts, download, upload, communicate or pass on, material, remarks, proposals or comments that relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003					X
	Possession of extreme pornographic image (grossly offensive, disgusting or otherwise obscene in character) Contrary to the Criminal Justice Act and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including the promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using the school system to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information e.g. financial information, databases, computer/network access codes and passwords					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading/uploading large files that hinders other users in their use of the internet)					X	
On- line gaming (educational)			X			
On Line gaming (non-educational)				X		
On line gambling					X	
On line shopping/commerce					X	
File sharing		X				
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube			X	X		

Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to school networks, data and files, through the use of computers/devices
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

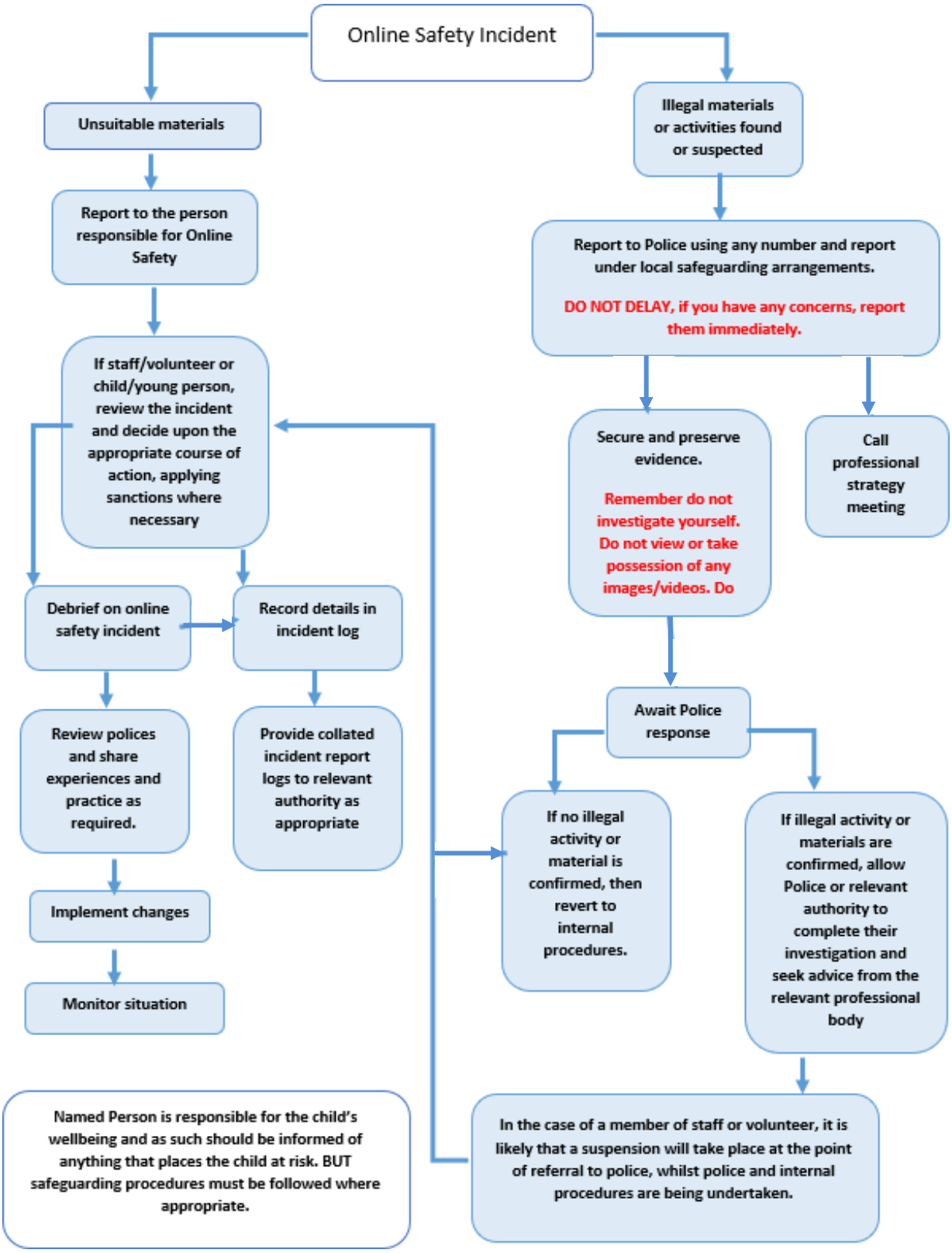
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see User Actions above). An incident management flow chart is included as a guide on how to respond to incidents of misuse.

Illegal incidents

If there is any suspicion that the website/s concerned may contain child abuse images, or if there is any other suspected illegal activity, the right-hand side of the flow chart should be referred too. A report should be made immediately to the police

.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number 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 view or take possession of any images/videos. Do
Call professional strategy meeting
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.

Other incidents

It is hoped that all members of the Galileo community will be responsible users of digital technologies, who will understand and follow school policy. However, there may be times when infringements of the policy could take place, through carelessness or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one member of staff/volunteer involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the safe computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 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 (except in the case of images of child sexual abuse)
- 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 the LA or national or local organisation as relevant
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:
    - Incidents of grooming behaviour
    - The sending of obscene material to a child
    - Adult material which potentially breaches the Obscene Publication Act
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Galileo Schools Actions and Sanctions

It is more likely that schools 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 as follows:

All incidents involving pupils should be logged on CPOMS under online safety tab with DSL.

Pupil Incidents	Refer to class teacher/tutor	Refer to SLT/Headteacher	Refer to Police	Refer to technical support staff	Inform parents/carers	Removal of network access	Warning
Deliberately accessing or trying to access material that could be considered illegal		X	X	X	X		
Unauthorised use of non- educational sites during lessons	X	X					
Unauthorised/inappropriate use of mobile phone/digital camera/ other mobile device	X	X			X		
Unauthorised/inappropriate use of social media/messaging apps/personal emails		X					
Unauthorised downloading or uploading of files		X		X			
Allowing others to access school network by sharing username and passwords		X		X			
Attempting to access or accessing the school network using another pupil's account		X		X	X		
Attempting to access the school network using the account of a member of staff		X		X	X		
Corrupting or destroying the data of other users		X			X	X	
Sending an email, text or message that is regarding as offensive, harassment or of a bullying nature	X	X	X		X		X
Continued infringement of the above, following previous warnings or sanctions		X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		
Using proxy sites or other means to subvert the school's filtering system		X	X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X	X	
Deliberately accessing or trying to access pornographic material		X	X	X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X					

Staff Incidents	Refer to Headteacher CEO (for central staff)	Refer to Central Exec. Team	Refer to Police	Refer to technical support	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X	X				
Inappropriate personal use of the internet/social media/personal email	X						
Unauthorised downloading or uploading of files	X						
Allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network using another person's account	X						
Careless use of personal data e.g., holding transferring data in an insecure manner	X						
Deliberate actions to breach data protection or network security rules	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X					
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with students	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 of the ethos of the school	X	X					
Using proxy sites or other means to subvert the school's filtering system	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X				
Breaching copyright or licensing regulations	X			X			
Continued infringements of the above following previous warnings or sanctions	X	X					