Acceptable User Policy

Schedule for Development/Monitoring/Review

This Policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	
The implementation of this Acceptable Use Policy will be monitored by the:	*Head Teacher* *School Business Manager* *Teachers*
Monitoring will take place at regular intervals:	*Annually*
The Board of Directors/Governing Body/Governors Sub Committee will receive a report on the implementation of the Acceptable Use Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Acceptable Use Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering by Esafe
- Surveys/questionnaires

All staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Acceptable Use Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head Teacher for investigation/action/sanction
- all digital communications with pupils/parents/carers should be 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 Acceptable Use Policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils:

With the support of Epinay staff:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- where appropriate, 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/use of images and on online-bullying.
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the Acceptable Use 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 that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and

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 images taken at school events
- access to parents/carers sections of the website and online student/pupil records
- the use of social media sites

Policy Statements

Digital Citizenship – Pupils

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, 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 Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and events
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of 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.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the 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/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Epinay School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities

- Letters, newsletters, our school website
- Parents/Carers evenings
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in the use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their Online Safety provision

Staff

Staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered periodically to keep staff up to date with technological advancements.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

Our school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that 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 recommended technical requirements through the SLA with ICT in Schools Team.
- There will be regular reviews and audits of the safety and security of 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. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the school ICT systems, used by the Network Manager must also be available to the Head Teacher or other nominated senior leader and kept in a secure place.
- Technicians are 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 the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes - logging requests with the school office to be managed by ICT in Schools team.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users – staff/pupils/etc).
- Activity of users on the school technical systems is monitored 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, work stations, mobile devices 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. trainee teachers, supply teachers, visitors) onto the school systems.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet and G Suite for Education.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before images of pupils are published on the school website/social media/local 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 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 others in the digital/video images.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that 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.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with images.

Use of portable storage devices (drives and memory pens)

Epinay school does not allow the use of portable storage unless by authorisation from the Head Teacher. Cloud storage is the preferred method.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and Epinay School's Data Protection Policy.

Staff must ensure that they:

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

Communications

Epinay School allows:

	School Devices	Personal Devices		
	School owned for single user	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*No*	*No*	*No*
No network access	*Yes*	*Yes*	*Yes*	*Yes*
Use of social media	*Certain staff*	*No*	*Yes*	*Yes*

Protecting Professional Identity

Our school and local authority have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information 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

School staff should ensure that they follow the staff Acceptable Use Policy at all times.

Responding to incidents of misuse

Epinay School follows the LA Reporting of Incidents as shown in Appendix ii.

Appendices

Appendix i) - Acceptable Use Policy Agreement

Appendix ii) - Responding to Incidents

Appendix iii) - Other Incidents

Date approved:	Nov 2020
Date Reviewed:	Nov 2021

Appendix i)

Student/Pupil Acceptable Use Agreement – to be displayed on ICT equipment and in areas within school.

I will not use the computer without permission.

I will check with an adult before using the Internet or e-mail.

I will not give away any personal details, including passwords.

I will not click on e-mail addresses shown on websites.

I will not download anything from the Internet without permission.

I will tell an adult if I see anything unpleasant.

I understand that the school may check my computer files and may monitor the Internet sites I visit.

I will not use my own disks or pen drives.

I know that all my communications with other people using ICT should be polite and friendly and will not deliberately send anything unfriendly or nasty.

For Parents/Carers Consent - To be included on parent/carers school consent form and included remote learning policy

Staff Acceptable Use Policy Agreement

- I have received (have access to a central copy) a copy of the school's E-Safety/acceptable use policy.
- I will only use the school's e-mail/Internet/Network/Personal e-mail for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only log onto the school Network/Internet using an assigned user account, set up by the school technician by prior request and will not log on with anyone else's individual details. (Group accounts for children should only be used when necessary to set or retrieve work.)
- I will log off from my account when it is not in use to prevent access by unauthorised pupils/staff.
- I will ensure that the pages of my personal social networking sites (Facebook/Twitter etc) that I am a member of are of an appropriate nature and that the pages of any 'friends' that I am linked to are also appropriate. Staff have a professional responsibility to ensure personal information is kept private and any references to school are not communicated via social networking sites.
- I will ensure that I will only use Facebook to update the school site. I will not access my personal account at school.
- I will not engage in any online activity that may compromise my professional responsibilities. Staff must not agree to become 'friends' with any pupil currently at Epinay School. Should they be asked, they should decline and then discuss the reasons why not with their class in circle time/PSHE.
- I will not allow unauthorised individuals to access e-mail/Internet/the Network.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to a member of the e-safety team.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed. Any downloads should be approved by the school technician.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network/Internet that does not have an up-to-date version of antivirus software.
- I will ensure I am aware of digital safe-guarding issues so they are appropriately embedded in my classroom practice.
- I understand that all Internet usage will be logged and this information could be made available to my Head Teacher on request.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

Signed_____Date_____

Appendix ii)

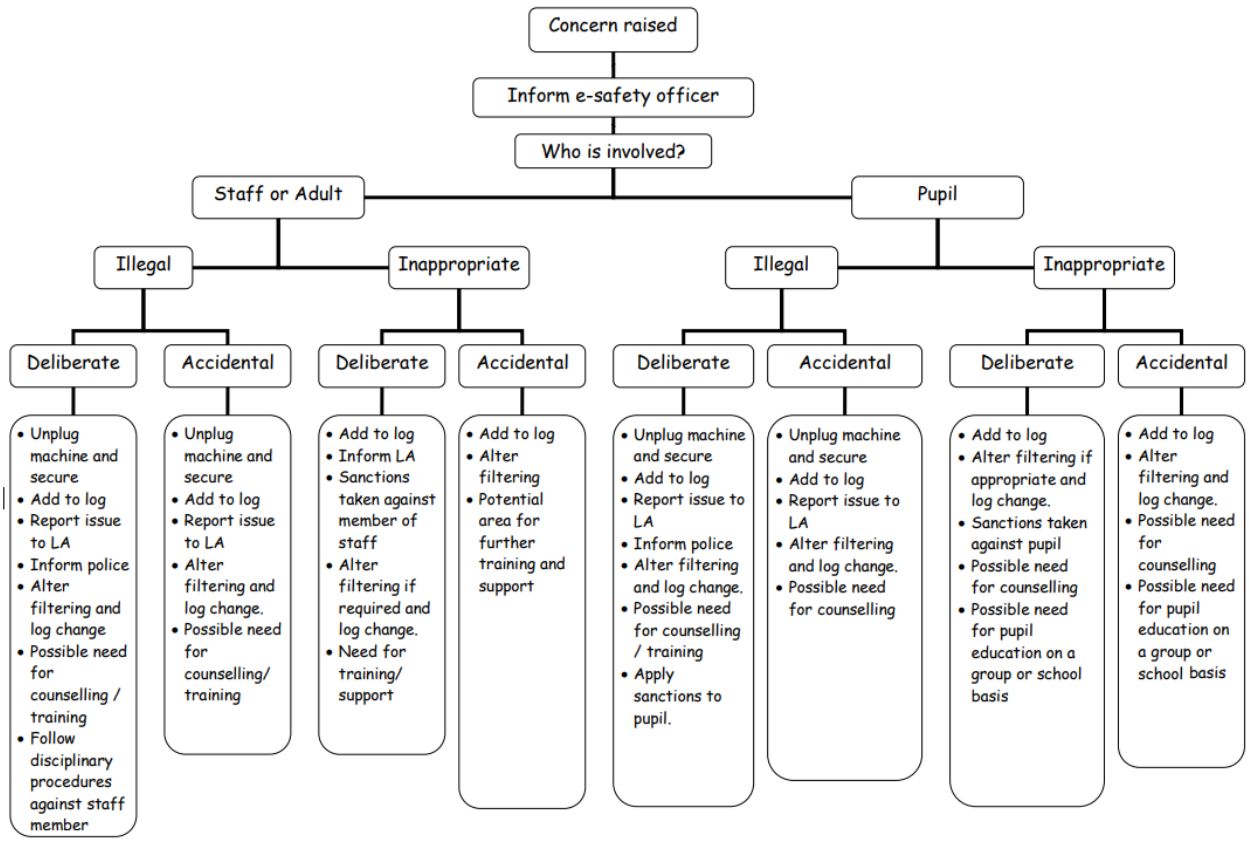
Reporting an E –Safety Incident – Guidance

Introduction

E-safety incidents can take many forms; from the accidental access of inappropriate content to serious incidents including illegal images or behaviours by adults or children.

The flow diagramhow dealing with an e-safety incident is designed as a guidance document to help you ascertain how to respond to an incident, actions you need to take and who to involve. These processes will be reviewed regularly to help ensure you have the appropriate support and information to ensure you act appropriately when incidents arise. We welcome your feedback and encourage you to share this with, in the first instance, Mike Hamilton, who is the LA lead for ICT and based at The Word.

Schools do need to be clear in their understanding of the differences between 'inappropriate' and 'illegal' content. Examples of inappropriate content can include soft porn (e.g. 'page three' images), political extremism and online gaming whilst illegal content would include cyberstalking or harassment; internet fraud; dangerous and illegal activities, such as bomb-making, terrorism, or unlicensed trade in weapons; physical threats; hate crimes, such as advocating genocide or violence; copyright violations; hacking: illegally breaking into individual computers or computer networks; child pornography. The school will need to take a view on whether access is deliberate or accidental.



The E-Safety Officer Role

All schools should identify a member of staff to take on the role of e-safety officer. Many schools choose the person who already has a responsibility for child protection, and some identify the Head Teacher as this can be a very challenging area when serious incidents occur. It is important that whoever is identified has the experience and confidence to respond appropriately when required - and when that person is unavailable, another member of staff can take on this role.

In all instances of an e-safety incident the e safety officer should be notified and log the details in the school's e-safety incident book. By logging even accidental incidents this will help inform filtering policies, AUPs and education and training needs within the school.

Schools should keep a record of the reporting process for each incident to help document that they reported the incident to the appropriate individuals and organisations. The E-Safety Officer should report access to illegal websites via school's systems to the Local Authority E-Safety Contact for Schools.

Adults (including teachers, assistants, governors, visitors etc.)

Where illegal content is accessed deliberately or accidentally the incident needs to be logged, reported to the Head Teacher and the local authority. Where the incident is believed to be deliberate, the school must also notify the police but must ensure that the Local Authority are informed first.

Although illegal sites are filtered it is unlikely that either a child or an adult will access them accidentally. Having said this, it is a remote possibility that an illegal site displaying child abuse imagery or other illegal images not yet listed with the Internet Watch Foundation is not filtered and a genuine accidental incident could occur. In some extreme cases the police may need to be informed of accidental access to illegal material; the Local Authority contact will advise schools on the appropriateness of this action when the incident is reported to them. For other illegal content the computer should be isolated and the images etc. not shared with anyone until the correct procedure is followed, reported and recorded.

In either accidental or deliberate cases the equipment will need to be isolated and the local authority or police will arrange for further examination of the device. The local authority will provide assistance in adjusting the in-school filtering and provide further training, support and guidance.

Where inappropriate content is accessed accidentally the filtering policies can be amended and further training and support provided if required. In the case of deliberate access, the school should follow established disciplinary procedures, amend filtering and notify the local authority. The local authority will then follow their procedure for reporting.

Children and Young People

The reporting processes remain the same as those for incidents relating to adults. Where illegal activity has taken place accidentally or deliberately, the device needs to be isolated, forensically analysed and restored prior to using again within the establishment.

In the case of either deliberate or accidental access to illegal content it is likely that the person will need counselling and support within school and other agencies. The local authority will be able to assist with identifying this.

Where a child or young person has deliberately or accidentally accessed inappropriate content there is an opportunity to provide further education to the individuals involved and the students. The local authority can provide in-school support and provide information on other sources of information and teaching and learning resources.

In each instance it is important to ensure that parents and carers are aware of the incident and encouraged to support the school's actions.

Illegal Content

Should you encounter something which you suspect to be illegal or suspect that a web site contains illegal material, contact the LA team immediately who will advise and support you. Please do not print out copies of offending information or forward it, or send links to anybody as the transmission of some content is a criminal offence itself.

IF the content is believed to be child abuse imagery they must immediately report it to the IWF as well as notifying the LA. No-one should be informed of the URL as no investigation must be made by anyone other than those licenced to view.

Further assistance is available by contacting Mike Hamilton ICTi n Schools Team The Word, 45 Market Place, South Shields

Key Contacts

Mike Hamilton (LA E-Safety Contact for Schools) Tel 0191 4246336

mike.hamilton@ictinschools.org

Beverley Shy (ICT & Information Security Officer) Tel 0191 424 7079

beverley.shy@southtyneside.gov.uk

Appendix iii)

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless 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 senior member of staff involved in this 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 same 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 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 (except in the case of images of child sexual abuse – see below)
- 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 Local Authority Group or national/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 materials to a child
    - adult material which potentially breaches the Obscene Publications 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 of 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.