**e-Policy – e-Safety in Internet Usage**

**Scope of the Policy**

This policy applies to all members of the school who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

**Policy Statements**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school’s e- safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

* A planned e-safety curriculum is provided as part of Computing / PHSE lessons
* Key e-safety messages will be reinforced as part of a programme of assemblies and pastoral activities
* Students are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
* Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Students will be encouraged to adopt safe and responsible use both within and outside school
* Staff should act as good role models in their use of digital technologies the internet and mobile devices
* In lessons where internet use is pre-planned, it is best practice that students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
* Where students 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, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff will pay particular attention and will monitor sites being researched.

Proscribed Activities – Internet Activities NOT permitted



**Schedule for Development / Monitoring / Review**

The school will review the possibilities to monitor the impact of the policy using:

* Logs of reported incidents
* Monitoring logs of internet activity (including sites visited)
* Internal monitoring data for network activity

**Roles and Responsibilities**

The following section outlines the e-safety responsibilities within the school

Head-teacher

* Acts as e-Safety Officer (supported by IT Lead)
* A duty of care for ensuring the safety (including e-safety) of members of the school community,
* The procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
* That there is a system in place to allow for monitoring and support of those staff in school who carry out the internal e-safety monitoring role. (This is to provide a safety net and also support to those colleagues who take on important monitoring roles.)
* Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
* Provides training and advice for staff
* Liaises with the Local Authority where appropriate
* Receives/creates log/reports of e-safety incidents inform future e-safety developments,

Designated Safeguarding Lead and Deputy (DDSL)

are trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

(nb. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop)

Teaching and Support Staff

* + they have an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices
	+ they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
	+ all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
	+ e-safety issues are embedded in all aspects of the curriculum and other activities
	+ students / pupils understand and follow the e-safety and acceptable use policies
	+ students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
	+ Staff 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 students / 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

Students

* are expected to read, and sign to confirm their understanding and agreement of the Tutorial “Pupil Acceptable Use Agreement”.
* are responsible for using the school digital technology systems and aware that it is not permitted to view or share Internet searches with any sexual, racial or potentially radicalising content
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand 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 cyber-bullying.
* should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s / academy’s E-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 that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers are encouraged to support the school in promoting good e-safety practice and use of:

* + digital and video images taken at school events
	+ their children’s personal devices in the school (where this is allowed)

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line 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. The school will therefore seek to provide information and awareness to parents and carers where this is appropriate

**Technical – infrastructure / equipment, filtering and monitoring**

The Tutorial Foundation (TTF) has a managed ICT service provided by an outside contractor.

The Tutorial Foundation ensures that the managed ICT service provider is fully aware of the school / academy e-safety policy and procedures, and carries out all the e-safety as suggested below.

* the school’s technical infrastructure is secure and is not open to misuse or malicious attack
* the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / 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 (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
* that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
* that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation
* that monitoring software / systems are implemented and updated as agreed

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

The Tutorial Foundation technical systems will be managed in ways that ensure that the school provides a safe technical environment for staff and pupils to work in

* There will be regular reviews and audits of the safety and security of school academy 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 the IT administrator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
* The “master / administrator” passwords for the school ICT system, are kept securely in the school admin office
* The IT administrator 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
* Internet access is filtered for all users. Illegal content (child sexual abuse images) 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. (the school / academy will need to decide on the merits of external / internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
* School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (schools may wish to add details of the monitoring programmes that are used).
* Any actual / potential technical incident / security breach should be reported to the Headteacher/DSL.
* 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 (IT Usage Policy) regarding:
	+ the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
	+ forbids staff from downloading executable files and installing programmes on school devices without express permission.
* Policy Sign off and review

|  |  |  |
| --- | --- | --- |
|  | **By whom** | **Date** |
| **Policy signed off by** | Julia Low | 15.01.16 |
| **Reviewed by** | Christopher Grant | 25.11.2021 |
| **Next Review By** | Julia Low | 30.11.2022 |

 **Appendix – Additional Resourses / Contacts**

Excellent Additional Guidance and resources provided by SWGfL

<http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy/Content/ESP_template-School-Template-Policy.aspx>

Advice may be obtained from the Child Exploitation & Online Protection agency CEOP, contact details via the link below. CEOP “Ambassador” courses are available

<https://ceop.police.uk/safety-centre/>