Policy Name:	Online Safety
Policy Date:	November 2019
Review Frequency:	3 Years

Online Safety

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, governors) 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 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 cyberbullying or other Online 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. 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 Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

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 Online Safety Co-ordinator.

The Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Coordinator:

The Online Safety Coordinator takes day to day responsibility for online safety issues and has a

leading role in establishing and reviewing the school online safety policies / documents.
In addition they:

Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
provide training and advice for staff
liaise with school technical staff receive reports of online safety incidents and create a log of incidents to inform future online safety developments

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:
♣ that the school's technical infrastructure is secure and is not open to misuse or malicious attack
♣ that the school meets required online safety technical requirements and any Local Authority 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 its 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 is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Coordinator for investigation and action that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

♣ they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
♣ they have read, understood and signed the Staff Acceptable Use Policy
♣ they report any suspected misuse or problem to the Headteacher /Online Safety Coordinator for investigation
♣ all digital communications with pupils / 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 Online Safety Policy and acceptable use policies
♣ 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.

Designated Safeguarding Lead:

Should be trained in Online 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

Pupils, as age appropriate:

♣ are responsible for using the school 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 / use of images and on cyber-bullying.
♣ should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 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 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 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.

Education – Pupils

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. Children need the help and support of the school to recognise and avoid online safety risks 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, 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. 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.

Education – Parents / Carers

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of their children's on-line behaviours. Parents may underestimate how often children 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 through:

♣ Letters, newsletters, web site
♣ High profile events / campaigns e.g. Safer Internet Day
♣ Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

It is essential that all staff 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 existing and new staff. This will be regularly updated and reinforced.
♣ The Online Safety Coordinator will receive regular updates through attendance at external training and by reviewing guidance documents released by relevant organisations.
♣ The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school, along with 123ICT, 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 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.
♣ 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 administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated school staff and kept in a secure place.
♣ The Network Manager 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. Content lists are regularly updated and internet use is logged and regularly monitored.
♣ Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
♣ An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Network Manager.
♣ 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.

♣ 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.

♣ An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be provided by the school and might include: iPad, tablet, laptop that usually has the capability of utilising the school's wireless network. All users should understand that the primary purpose of the 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.

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 photographs of pupils are published on the school website / local press.

Parents / carers are welcome to take digital images of their children at school events for their own personal use, where possible a recording will be taken and made available to parents. To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims. These 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.

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' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communications

When using communication technologies the school considers the following as good practice:
The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email addresses to communicate with others when in school, or on school systems (e.g. by remote access).

Users must immediately report, to the DSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff and pupils or parents / carers (email, blogs etc) must be professional in tone and content

Pupils should 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 Actions & Sanctions

It is more likely that the school 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 in accordance with the school behaviour policy and if necessary, the LADO (Local Area Designated Office) if related to a member of staff.

Signed: _____ (Signed version to be found onsite at Grendon Underwood School)