Grateley Primary School

***A school where every child becomes a lifelong learner and realises their potential*.**

E-Safety Policy

Reviewed: February 2019
Next review: February 2020

Signed: Chair of Governors: Amelia Bridges

Rationale

Safeguarding (including online safety) is the responsibility of everybody who works within the school.
The KCSIE (September 2018) document identifies that education settings are responsible for ensuring that:

- appropriate filtering and monitoring of internet access is in place
- all members of staff receive appropriate training and guidance
- the curriculum prepares children for the digital world.

There should be a designated online safety lead (Head teacher) who keeps up to date with new technologies and builds awareness with stakeholders about how they can remain safe. Online safety concerns may cross into the child protection threshold so the DSL needs to understand the role other agencies might take.

The DSL (online) (Head teacher) should:

- Act as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety.
- Coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with current GDPR legislation.
- Maintain a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. (**It is recommended that schools and settings record online safety within existing child protection/safeguarding procedures and files to achieve this**)
- Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- Report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaise with the local authority and other local and national bodies, as appropriate.
- Work with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensure that online safety is integrated with other appropriate school policies and procedures.

Responsibilities of all Staff

All staff are responsible for safeguarding children on and off line. Their key responsibilities are:

- Contributing to the development of online safety policies
- Reading and adhering to Acceptable Use Policies (AUPs)
- Taking responsibility for the security of school/ setting systems and data
- Having an awareness of a range of different online safety and how they relate to safeguarding children. This should include sexting and cyberbullying.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures
- Knowing when and how to escalate online safety issues, internally and externally
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

Responsibilities of Staff managing the technical environment

Staff managing the technical environment have an essential role to play in establishing and maintaining a safe online environment. Staff with technical responsibility should:

- work closely with the school leaders, Designated Safeguarding Lead (DSL) as well as pastoral and curriculum staff (where appropriate) to provide expertise relating to appropriate education use of ICT systems and also to ensure that learning opportunities are not unnecessarily restricted by technical safety measures.
- be clear about the procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the DSL and/or Head teacher/manager in line with existing school/setting safeguarding policies.
- Ensure that an external service provider upholds the online safety practices including referring any concerns to the online safety coordinator or leadership team.
- Ensure that the school network is monitored and any concerns reported to the DSL
- Develop an understanding of the relevant legislation
- Ensure that the school's ICT infrastructure is secure but not so secure that it gets in the way of learning.

- Ensure that appropriate anti-virus software and system updates are installed and maintained on all electronic devices.

Responsibilities of Children and Young People

Young people should take responsibility and take ownership of any online safety policy. They should:

- Contribute to the development of these policies
- Read the school Acceptable Use Policies (AUP) and adhere to them
- Respect the feelings and right of others both online and offline
- Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues
- Take responsibility for keeping themselves and others safe online
- Take responsibility for understanding risks posed by new technologies
- Assess the personal risk of using any particular technology and behave safely and responsibly to limit those risks.

Responsibilities of Parents/ Carers

Parents and carers should:

- Read the school Acceptable Use Policies (AUP), encourage themselves and their children to adhere to them
- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role model safe and appropriate uses of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Staying safe when using Online Communication

Website:

Grateley Primary School considers what information is published on the school's public website as opposed to a password protected online area. The following link provides the detail, the DfE have provided about what should be found on the website: https://www.gov.uk/what-maintained-schools-must-publish-online

Publishing images and videos online:

Written permission from parents and carers is sought through a standard parental permission from completed by parents before images/ videos are posted online. These should only be posted in consideration of other safeguarding and data protection policies.

E-mail:

Personal email should not be used in the school setting. School emails are used for all communications in a professional context. Staff are made aware that these emails are not private and can be monitored. The risk of sharing data via school email is always considered. Grateley school takes careful consideration of the confidentiality of the data as well as a work life balance; staff are discouraged in sending emails out of hours.
Schools should consider the naming convention of emails to guard against a young person being identified. When using external email providers like Google Apps schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits. Schools must ensure that these providers abide by the data protection act. Professionals must ensure that their use of email at work always compiles with GDPR data protection legislation and confidential or personal data must not be sent electronically via email unless it is encrypted. Staff are appropriately trained and the leadership team ensure that all members of staff use appropriately secure email systems to share any sensitive or personal information.

Classroom use of the Internet:

Staff are made aware that no search engine or filtering tool is ever completely safe, and appropriate supervision, use of safe search tools, pre checks of search terms, age appropriate education for pupils and robust classroom management must be in place. However there is still always a risk that children will be exposed to inappropriate content. The quality of information on the internet is variable. Staff and students are made aware of how they can critically evaluate the information available. Devices that children may bring into school should be risk assessed and supported with clear policies, procedures and training.

Social Media:

There are significant benefits for communication, engagement, collaboration and learning via the internet and social media however alongside this there are risks associated with users such as staff, pupils and the wider school community. There are many tools that can be used to communicate online with applications like Facebook, Instagram and snapchat as well as numerous apps published on a daily basis. These sites are at risk of being exposed to a great deal of advertising and could provide access to inappropriate content. Pupils should be made encouraged to limit the amount of personal information they upload and some of the risks of sharing this information.

Staff personal use of social media :

'Keeping children safe in education' 2018 highlights that Governing Bodies and proprietors need to ensure that their settings have a "…a staff behaviour policy (sometimes called the code of conduct) which should amongst other things include – acceptable use of technologies, staff/pupil relationships and communications including the use of social media." It is therefore essential that schools ensure all members of staff are aware of professional boundaries regarding both their 'on' and 'offline' communication.

Schools cannot ban staff from using social media but they should offer advice and guidance to ensure that staff remains safe and maintain the necessary professional boundaries.

All staff need to be aware:

- Of the importance of considering the material they might publish online so that it doesn't undermine the professional reputation of themselves or their schools which could result in a disciplinary issue.
- That they should use the highest privacy settings when social networking
- Not engage in communication with present or past pupils or parents of these pupils unless there is a justifiable professional reason.

If it is seen as beneficial for staff to communicate with pupils this should be set up through an official establishment social networking page including members of the senior leadership team. These need to provide clear areas of transparency. If there are any pre-existing relationships these should be declared to the DSL to formally acknowledge the relationship.

The following links may be helpful to share with members of staff:
www.childnet.com/teachers-and-professionals/for-you-as-a-professional
www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation
www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation
www.saferinternet.org.uk/about/helpline/faqs

Pupils use of social media:

Grateley Primary School has a responsibility to ensure that pupils in the school have been provided appropriate education around the safe use of the internet and social media. This is part of the Computing programme of study but is also be part of the PSHE curriculum.

Many sites have a restriction of age 13. It is not illegal for pupils under this age to access these sites it's just not recommended because of the risk of them being targeted with unsuitable advertisements.

If children are using social media sites inappropriately (such as cyberbullying, posting personal information, adding strangers as friends etc.) or there are other safeguarding concerns due to vulnerabilities etc., then the school/setting should respond to the concern in line with existing policies, for example anti-bullying, child protection/safeguarding or behaviour policy. If a child is at risk of significant harm then the DSL must be informed and the existing child protection procedures should be followed.

Use of Personal Devices and Mobile Phones:

As with many forms of technology mobile phones and personal devices are undergoing constant development with increased functionality. They are multifunctional tools that are becoming essential in personal and work life. However they can present problems such as:

- Items that can be stolen and damaged

- Used for bullying
- Internet access that can bypass school monitoring and filtering
- Undermine class discipline
- Breach data protection and confidentiality policies
- The use of images to bully

Under the EYFS, all early years settings and foundation stage providers must have a clear safeguarding policy which covers the use of mobile phones and cameras in the setting.
In the context of mobile phones schools should ensure that:

- Teaching, learning and behaviour should not be impeded
- Staff should be given clear boundaries on professional use and expectations,
- Learners should be given explicit education regarding appropriate use of mobile phones and personal devices

The Head teacher and Governing Body will consider the risk to data protection if they allow staff to use their personal devices for their professional role. Strategies are implemented to safeguard this data. This should include:

- Use of passwords
- Data encryption
- Awareness around GDPR regulations
- Awareness of Acceptable Use Policies

Any use of mobile or handheld devices should be risk assessed with the involvement of all stakeholders including parents and pupils.

Staff use of personal devices and mobile phones:

School leaders and managers have identified school expectations regarding appropriate and proportional staff use of personal devices to access school content e.g. school email, learning platforms and have identified expectations for safe use to ensure possible risks can be mitigated. Staff are actively discouraged from using their personal devices for recording images and video.
School leaders are aware that seizing and searching members of staffs' personal devices may be unlawful. If leaders feel this is required or appropriate, for example if a criminal offence may have been committed, then the appropriate agency should be informed. The DSL may wish to seek advice from the Education Safeguarding team who can be contacted at hscb@hants.gov.uk or the LADO (Local Authority Designated Officer) if there has been an allegation against a member of staff.

- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school/setting policy then disciplinary action will be taken.

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

Policy Decisions

Reducing online risks:
Devices are being produced with increased functionality which could pose problems for staff in the context of behaviour management. Staffs are regularly trained on new technologies and the school undertakes a risk assessment for any new technologies that we are considering introducing as a communication or teaching and learning.

Authorising internet access:
All students and staff should are provided with internet access to support educational outcomes. If there are concerns about the well-being of a child – the child's internet access will be removed in alignment with the school's behaviour policy.

Monitoring and Review

The implementation of the E-Safety policy will be monitored by:

Deputy Head Teacher as Computing and ICT leader/Anti-bullying co-ordinator
Head Teacher
Governing Body
Designated Safeguarding Lead

The policy will be reviewed annually, or more regularly in light of any new technological developments or incidents that may have taken place, both within the school or nationally.

The school will monitor the impact of the policy by:

Reviewing the log of reported incidents
Surveying pupils, parents and staff.

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, and community users) who may have access to school systems, data or school equipment at any time, including hardware and software. This policy also applies all other ICT equipment brought onto the school premises by staff. On the rare occasion of any equipment being brought into school, it should be arranged with the head teacher in advance.

Any incidents arising out of the policy will be dealt with and the school will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour in school and out of school where appropriate.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors:
Governors are responsible for the approval of the e-safety Policy and for reviewing its effectiveness. This will be carried out by the School Improvement Committee.

Head Teacher and Leadership Team:
The Head teacher is responsible for the safety, including e-safety of all members of the school community, although day to day responsibility will be assigned to the ICT Co-ordinator.
The Leadership Team are responsible for ensuring the ICT Co-ordinator and other relevant staff receive suitable training or CPD in order that they can carry out their roles and train other colleagues as relevant.

ICT Co-ordinator/Deputy Head Teacher
Lead E-Safety within the school.
Take day to day responsibility for e-safety issues, including providing training and advice to staff.
Monitor e-safety incident and report regularly to the Leadership Team.
To liaise with the local authority when necessary.

All Teaching and Support Staff

- Have an up to date awareness of e-safety matters, including current policy and practices - including The Prevent Strategy;
- Report in writing any concerns over cyber/online issues to the HT.
- They have read, understood and signed the Responsible Internet/Digital Technology Use Statement; Safeguarding/Child Protection and associated policies
- Understand that under no circumstances are they to provide pupils with their email/social media/mobile phone devices etc.;
- Ensure that all children in their care understand how to keep themselves safe online through ongoing class discussions, assemblies and PHSE/PDL lessons and internet/cyber safety lessons;
- Report in writing any suspected misuse or problems to the ICT Co-ordinator for investigation/action/sanction as soon as is possible and usually on the day of the concern being raised;
- Ensure pupils understand and follow the school e-safety Pupils Rules for Responsible Internet/Digital Technology Use.
- Ensure pupils have a good understanding of research skills
- Monitor ICT activity closely during lessons.
- Pre-plan internet based lessons to check sites are suitable for pupils’ use - reporting and/or blocking any sites/pop-up etc. that may be unsuitable.

Pupils:

Responsible for using the school's ICT system in accordance with the Pupil Rules for Responsible Internet/Digital Technology Use

Understand and uphold copyright regulations.

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Respond appropriately to issues relating to e-safety and cyber bullying and report any concerns to an appropriate member of staff,

Understand the importance of adopting good e-safety practice, when using digital technology in and out of school.

Parents:

Ensure that their children use internet and mobile devices in an appropriate way.

Inform the school of any e-safety issues relevant to their child e.g. cyber bullying incidents.

Ensure that they follow the legal guidelines for use of on-line sites, social media etc. e.g. legal ages/levels of supervision

School Wide Digital Technology Management

The Head Teacher will delegate editorial responsibility of our school website to the Admin Officer, in liaison with the Deputy Head teacher, to ensure that content is accurate and quality of presentation is maintained.

The website will comply with the school's guidelines:

Photographs must not identify individual pupils, other than by first name and where permission has been granted beforehand.

Written permission from parents will be sought before photographs of pupils are published on the school website, media or in school publications.

Parents will be informed that pupils will be provided with supervised internet access and will sign the appropriate agreements before their child can use the internet or school technologies,

Personal CD's may be brought into school by pupils, but their use would be supervised and conducted after appropriate virus checks;

Personal memory sticks may not be brought into school by pupils. Staff may use memory sticks for planning/work preparation, however these must be stored in lockable storage and must not under any circumstances be left out/in computers during the school day. No pupil/staff/family details may be kept on memory sticks other than the school encrypted backup.

Responsibility for handling incidents will be given to the Deputy Head teacher in liaison with the Head Teacher.

The ‘Responsible Internet Use Statement’ or ‘Rules for Responsible Internet Use’ signed by staff and pupils (see appendix 1 and 2);

Rules/Guidelines for internet access will be posted near computer systems and laptop trolleys. (See appendix 3)

All staff, including teachers, supply staff, teaching assistants and support staff will be provided with the E-Safety Policy and its importance explained;

Parents' attention will be drawn to the policy in newsletters, the school prospectus and on the school website;

<u>The Internet</u>

Aims of use:

To give pupils and staff the opportunities to:

- access world-wide educational resources
- to become astute and critical users of information
- participate in new initiatives such as a managed learning environment
- gather information and have cultural exchanges between appropriate pupils in other schools
- participate in staff discussions with experts in many fields
- provide access to educational materials and good curriculum practice
- communicate with the advisory and support services, professional associations and colleagues
- exchange curriculum and administration data with the Local Authority (LA) and Department for Education (DfE)

<u>Planning and use of the Internet</u>

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement.

Pupils will be given clear objectives for internet use.

Staff will select sites which will support the learning outcomes planned for the pupils’ age and maturity.

Approved sites must be bookmarked, listed or copied to the school intranet.

Staff and pupils will not be allowed to access public chat rooms, including social network sites.

Staff and pupils will not access inappropriate sites that could put others at risk, and if inappropriate sites are encountered accidentally they will be reported to a member of the ICT team.

New facilities will be thoroughly tested before pupils are given access.

Internet access will be granted to a whole class as part of the scheme of work after a suitable education in responsible internet use;

Pupils using the Internet will be supervised by an adult;

If staff or pupils discover unsuitable sites, the URL (address) and content will be immediately reported to HCC via the administration officer. Children must then be directed away from the site and prevented from accessing this again.

Teaching Safe Use of the Internet

Teaching children to be safe users of the internet is of prime importance. Children before every lesson will be briefed in how to access the internet in a safer way. They will be also be reminded what to do if they see material that upsets or disturbs them, or in anyway makes them feel uncomfortable.

Class teachers, following advice from the ICT Co-ordinator, are responsible for ensuring that e-safety lessons are planned across the year.

National Links and Resources
Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings):
http://www.onlinecompass.org.uk/

Grateley Primary School

Responsible Internet /Digital Technologies Use Statement

Staff

The computer system/network is owned by the school and is made available to pupils to further their education and for staff to:

Enhance their professional activities including teaching, research, administration and management.

The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

Staff and pupils requesting internet access should sign a copy of our Acceptable Internet Use statement and return it to the ICT leader for approval.

Access should only be made via the authorised account and password, which should not be made available to any other person;

Staff may use memory sticks/mobile storage for planning/work preparation, however these must be kept safely remembering all the time that they may hold confidential information; any loss of such storage system may result in a breach of data protection and could result in a disciplinary action. If data storage system is compromised, staff must inform the head teacher immediately in order to minimise further risks.

Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;

Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;

Posting anonymous messages and forwarding chain letters is forbidden;

Copyright of materials must be respected;

All internet activity should be appropriate for staff professional activity or pupils' education.

The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded or may be sent inadvertently to the wrong person;

Use for personal financial gain, gambling, political purposes or advertising is forbidden;

Users must access only those sites and materials relevant to their work in school.

Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed;

Staff must not use their personal mobile phone/tablets or electronic devices in the school site (with the exception of the school office or staff room, or to make an emergency call on a school trip).

Under no circumstances are staff allowed to use their own cameras or camera phones, or take the school cameras home.

Staff must not give their email address/telephone numbers/or social media details to pupils or parents. Any e-contact must be made through school accounts.
Any material breach of this may result in disciplinary action.

Signed:____________________ Date:____________

Grateley Primary School

Rules for Responsible Internet/Digital Technology Use

Pupils

The school has computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

I will not open other people's files;

I will only use the computers for school work and homework;

I will only bring CD's into school with permission and supervision (we are not allowed to use Memory Sticks/storage devices);

I will ask permission from a member of staff before using the internet;

The messages I send will be polite and sensible;

I will not give my home address, telephone number, email address or personal website details, or arrange to meet someone, unless my parent, carer or teacher has given permission;

To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;

I will not use a mobile phone or electronic device on the school site

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

Signed by or on behalf of the pupil:__________________________

Date:______________________

Parent/Guardian Signature:________________________

Permission for Internet Access

Parent/carer's permission and pupil's agreement

I give permission for access to the Internet on the terms set out in the above letter.
I agree to follow the rules for Responsible Internet Use.

Signed: … … … …… …… …… …

Print name: … …… …… …… … …

Date: … …… …… …… …

Pupil Signed: … …… …… …… …… …

Print name: … …… …… …… … ……………………….. Class: … … …… …… …… … …