Grand Avenue Primary and Nursery School

Online Safety policy

Contents

Agreed by staff and Governors – Spring term 2020

Review date –Spring term 2023

Introduction/Aims

At Grand Avenue we believe that the internet and the World Wide Web are essential resources in supporting learning and teaching. We understand that computing plays an important role in our everyday lives and we accept our responsibility to teach our staff and pupils how to use technology safely.

The purpose of this policy is to ensure all members of our school community are aware of the need for online safety. It sets out the systems and procedures put in place to ensure all pupils, staff, governors and parents know how to stay safe when online.

This policy should be read in conjunction with other policies including child Protection, Safeguarding and Anti bullying.

Responsibilities and Procedures

Online safety for Pupils

All adults in school are responsible for ensuring pupils are kept safe when using the internet. Teaching staff are required to follow the online safety scheme of work, known as the 'Skills ladder'. This skills ladder sets out which aspects of online safety are to be taught in which year group and the main resources to be used. (See Appendix 1)

In addition to specific lessons on online safety, teachers are required to discuss and explain the Computing Code of Conduct at the beginning of each academic year and refer to this document periodically throughout the year. Pupils are asked to read and sign this document in September every year. Copies of the Code of Conduct for Computing are displayed in the ICT suite and in classrooms. (See Appendix 2)

Adults in school are responsible in ensuring pupils only use approved accounts on the school system. In addition to the Computing Code of Conduct pupils are reminded never to reveal details of themselves or others online and not to open attachments unless the author is known. The individual accounts have filters with regards to inappropriate language/comments and is tracked through the software such as ATOMWIDE and J2E.

Pupils will not be permitted to use social networking sites on school premises. However, safety guidance and age restrictions for these sites will be taught during online safety lessons and talks; for example, never give personal details and to use nicknames. Children will be encouraged to use a password checker to ensure that their password is of an adequate security level.

Online safety for Staff

All staff are required and expected to use technology sensibly, lawfully and professionally. All staff are required to read and sign two declarations; Acceptable Use and Transfer of Data with regards to use of ICT resources. The Computing co-ordinator will provide training in online safety guidance at regular intervals.

Online safety for Parents/Carers

On joining our school parents/carers are requested to read and sign a 'Home – School Agreement'. A copy of the policy is available for all parents/carers through our website. Further information can be found in our newsletters.

Parents who are aware of virtual or cyber bullying are encouraged to inform the school or the police as appropriate.

The school will maintain and make available to parents/carers a list of online safety resources to support parents in safeguarding their children online. (See Appendix 3)

Security

The ICT technician is responsible for reviewing the ICT system with regards to security. The Local Authority installs and updates virus protection (SOPHOS).

Filtering of websites and email is refreshed everyday by ATOMWIDE. Any reported unsuitable websites are reported to the Computing co-ordinator who will arrange for this website to be blocked.

Parents/carers are advised to use the school email address and telephone number as points of contact. Information regarding individual members of staff or pupils will not be published.

Written permission is sought from parents/carers in regards to the use of photographs of their children, this includes our school website. In any situation where photographs are used the child's full name will not be published.

When sharing work, learning videos and photos using the programme J2E, children will each have their own protected account that is monitored by teaching staff. Anything that is put forward to be shared has to be authorised by the class teacher and can only be shared with people in school. Children can comment on the work of their peers and these comments are monitored by J2E. Any inappropriate language or comments are blocked and the Computing coordinator is informed immediately. J2E are able to monitor and close accounts if they necessary.

Bullying

At Grand Avenue we deal with reported incidents of Virtual or Cyber bullying in accordance with our Anti bullying policy. (See Appendix 4)

We acknowledge that silent phone calls, abusive messages and comments on social networking sites can be very distressing and accept that this kind of bullying needs to be investigated and dealt with. The Computing coordinator will arrange online safety talks with the local authority advisor for children and parents so that they are aware of the steps to take if they receive anything distressing.

All incidents of Virtual or Cyber bullying will be reported to the Headteacher who will then take responsibility for the investigation and management of the incident. This

may include a meeting with parents or a letter outlining our concerns. The victim will receive appropriate support and if necessary the police will be informed of the situation.

Staff may seek further advice and support with regards to Virtual or Cyber bullying from their professional association or union.

Victims of Virtual or Cyber bullying are advised to;

- Save messages, texts, emails or posts
- Never to reply
- Block future messages
- Report the incident (Tell a trusted adult)

Prevention of Virtual and cyber bullying

All staff will be supported in their knowledge and understanding of the technologies pupils are using both inside and outside school. Regular training and updates will be provided by the Computing co-ordinator.

The subject of bullying (in all it's forms) will be a regular topic for assemblies, themed weeks and circle times.

Meetings for parents/carers will be organised to give information and advice

Pupils,staff , parents and Governors will be involved in evaluating and improving policies and procedures.

Complaints

All staff and pupils are asked to remain vigilant regarding the use of the internet on site and need to report any concerns regarding misuse to the Headteacher. The Headteacher will then arrange for the incident to be investigated . Should the incident involve child protection our designated child protection officer will be informed.

All reported incidents will be thoroughly investigated and parents/carers, staff and pupils informed of the consequences of such behaviour. This may include a ban on using certain technologies on our school site.

Concluding statement

At Grand Avenue we believe that all pupils and staff should have access to the internet and technologies regardless of race, culture, age, ability or gender. We endeavour to ensure that all access is monitored and that only appropriate resources are used on our school site.

APPENDIX 1 – Skills ladder

Online Safety Programme of skills scheme of work.

Year group	E-safety Programme	Skills
Reception	Hectors world. Lesson 1 and 2 http://wwwthinkuknow.co.uk/5-7/hectorsworld Song and introduction to characters.	I know not to use my real name on the internet. I know how to ask for help if I see something I don't like on the internet.
Year 1	Hectors world. http://wwwthinkuknow.co.uk/5-7/hectorsworld Lesson 3, 4, 5 and 6. Summer: - Introduce Lee and Kim's Adventure Coep 8min programme very important and lesson plan and activities included. http://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/	I know not to use my real name on the internet. I know how to ask for help if I see something I don't like on the internet.
Year 2	Autumn: - Revise and discuss Lee and Kim's Adventure Coep 8min programme very important and lesson plan and activities included. http://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/ ME ONLINE Log on to LGFL link Click on curriculum and then PSHE KS1 Click on ME ONLINE	I can send and open an email safely. I know how to tell someone if im unhappy about an internet page or email. I can report to CEOP any issues arisen from the use of the internet.
Year 3	Autumn: - Revising the rules and consequences and discuss Lee and Kim's Adventure Coep 8min programme very important and lesson plan and activities included. http://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/ The Smart Crew http://www.childnet.com/kia/primary/smartadventure	I understand the need for security online and will not open email attachments from unknown sources. I can communicate using e-mail or online discussion forums safely looking for the CEOP signs.
Year 4	https://www.lgfl.net/online-safety/resource-centre activities and lesson plans and instructions. Adapt lessons to your classes and year group needs	I am aware of safe ways to avoid identifying myself online. I am aware of the need for care in uploading information to the internet and

		downloading information.
Year 5	Autumn: - Jigsaw Film Lesson plan, prefilm activity 1 and 2 Watch film Post film activity 1& 2 Find film and resources under teacher files E-safety KS2 US online (new and improved) Log on to LGFL link Click on curriculum and then PSHE KS2 Click on US online 6 activities and lesson plans and instructions. Adapt lessons to your classes needs.	I know how to verify the authenticity of a website. I know how to report online incidents I find abusive.
Year 6	Autumn: - Jigsaw Film Revise and discuss from last year. Lesson plan, prefilm activity 1 and 2 Watch film Post film activity 1& 2 Find film and resources under teacher files E-safety KS2 Watch Where's Klaus? Discuss issues raised from this 4min clip. Lesson plan included. Download from http://www.thinkuknow.co.uk/teachers/resources Cybercafé http://www.thinkuknow.co.uk/8-10/cybercafe/ This includes lesson plans and discussion activities.	I am aware of safe behaviour and netiquette when using communal sites. I understand the consequences of cyber bullying and know that it comes in all different digital forms that can be tracked.

Computing Code of Conduct

STOP! Think Click

We only use the internet when an adult is present.

We only use websites our teacher has chosen.

We keep our usernames and passwords to ourselves.

We only click on buttons and links when we know what they do.

We only use search engines designed for children and when an adult is with us.

We always tell an adult when we get lost on the Internet.

We always tell an adult if we see anything that upsets us on the Internet.

My name: _____ Date: _____

Signature:_____

I

KS2 Computing Code of Conduct

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

In school I WILL	In school I WILL NOT
• Ask permission from a member of staff before using the Internet. • Only use the Internet for schoolwork and home learning. • Only e-mail people I know. • Only send e-mail messages that are polite, friendly and sensible. • Only open e-mail attachments from people I know. • Tell an adult straight away if I see anything I am unhappy with. • Tell an adult straight away if I accidentally click on something that I know I am not supposed to access. • Remember to log-out when I have finished using Network. • Leave my mobile phone in the school office.	• Access other people's computer files. • Download anything from the Internet without my teacher's permission. • Buy or sell anything, or enter any competition, whilst using the Internet. • Access websites that I know I am not allowed to use. • Give out my e-mail, home address, telephone number, or any other personal information. • Send my picture, or arrange to meet someone. • Send any other person's full name, home address, telephone number, picture, or other personal information, in an e-mail or over the Internet. • Use my phone. • Use social media. • Pretend to be someone else or lie about my age when I am using e-mail or the Internet.

I understand that the school will monitor my use of the School's Broadband Network, including all the Internet sites I visit, and may check my e-mails and computer files.

Should I break these rules my parent / carer will be told and I will not be allowed to use school ICT equipment.

My name: _____ Date: _____

Signature: _____

APPENDIX 3 – Resources for parents

Useful websites for Parents

http://www.childnet.com/safety/parents.aspx

Childnet have recently launched the digizen site, with information on cyberbullying and the dangers of Social Networking Sites:

The parentscentre website, has advice covering every aspect of Internet Safety for families

Other bodies providing advice, additional information, guidance and activities for children:

A CEOP site	Childnet International	Childnet International	CBBC Stay Safe	Childnet International	National Children's Homes

https://www.my1login.com/resources/password-strength-test/ This is a useful website in checking the strength of passwords. Your aim is to have a password that would take 10 million years to hack.

https://www.betterinternetforkids.eu/web/portal/onlineservices

https://www.net-aware.org.uk/networks/?order=title

These websites contain details on security settings for apps and websites. You can follow step by step guides on how to make sure that your child is as safe as they can be online.

Scan the codes below to get details on how to set parental controls on technology at home.

Using the Internet safely at home

Whilst many Internet Service Providers offer filtering systems to help you safeguard your child at home, it remains surprisingly easy for children to access inappropriate material including unsuitable texts, pictures and movies. Parents are advised to set the security levels within Internet Explorer with this in mind. Locating the computer in a family area, not a bedroom, will enable you to supervise children as they use the Internet. However, don't deny your child the opportunity to learn from the wide variety of material and games available on the Internet. Instead set some simple rules for keeping them safe and make sure they understand their importance.

Simple rules for keeping your child safe

To keep your child safe they should:

- ask permission before using the Internet
- only use websites you have chosen together or a child friendly search engine
- only email people they know. (why not consider setting up an address book?)
- ask permission before opening an email sent by someone they don't know
- not use Internet chat rooms
- not use their real name when using games on the Internet, (create a nick name)
- never give out a home address, phone or mobile number
- never tell someone they don't know where they go to school
- never arrange to meet someone they have 'met' on the Internet
- only use a webcam with people they know
- tell you immediately if they see anything they are unhappy with.

Using these rules

Go through these rules with your child and pin them up near to the computer. It is also a good idea to regularly check the Internet sites your child is visiting e.g. by clicking on History and Favourites. Please reassure your child that you want to keep them safe rather than take Internet access away from them.

For further information go to:

CEOP: www.ceop.gov.uk

Think U Know: www.thinkuknow.co.uk

Childnet: www.childnet-int.org

Some useful websites

When searching the Internet we recommend you use one of the following child friendly search engines:

Ask Jeeves for kids:
www.askforkids.com

Yahooligans:
www.yahooligans.com

CBBC Search:
www.bbc.co.uk/cbbc/search

Kidsclick:
www.kidsclick.org

Zoo Search:
www.zoo.com

Children, ICT & e-Safety

Information for parents and carers

The purpose of this guide

Children of today are increasingly using Information & Communication Technology (ICT) in schools and in the home. This guide explains:

- How your children are using ICT in school.
- How using ICT in the home can help children to learn.
- How children can use the Internet safely at home.
- Where to access further information.

How your child uses ICT at school

ICT in schools is taught as a subject in its own right and also supports children's learning in other subjects, including English and mathematics. Within ICT lessons children learn to use a wide range of ICT including:

- **Word Processing** to write stories, poems or letters
- **Databases** to record information, e.g. minibeasts
- **Spreadsheets** to create tables, charts and graphs
- **Desktop Publishing** to design posters, leaflets or cards
- **Multimedia Presentation** to present text, pictures and sound
- **Drawing Programs** to create pictures and designs
- **Internet and CD-ROMs** to find information
- **Email** to contact children and teachers in another school
- **Digital Cameras** to record what they have done in class or on a visit
- **Electronic Sensors** to record changes in light, sound and temperature
- **Controllable Robots** to give instructions and make something happen
- **Simulations** to explore real and imaginary situations
- **Website Publishing** to present ideas over the Internet.

How you can help your child at home

ICT is not just about using a computer. It also includes the use of controllable toys, digital cameras and everyday equipment such as a tape recorder or DVD player.

Children can be helped to develop their ICT skills at home by:

- writing a letter to a relative
- sending an email to a friend
- drawing a picture on screen
- using the Internet to research a class topic
- planning a route with a controllable toy
- using interactive games.

A selection of companies offer school software for use at home.

Benefits of using ICT at home

How we know that using ICT at home can help

Many studies have looked at the benefits of having access to a computer and/or the Internet at home. Here are some of the key findings:

- used effectively, ICT can improve children's achievement
- using ICT at home and at school develops skills for life
- children with supportive and involved parents and carers do better at school
- children enjoy using ICT
- using ICT provides access to a wider and more flexible range of learning materials.

How does learning at home using ICT benefit children?

Home use of ICT by children:

- improves their ICT skills
- offers them choice in what they learn and how they learn it
- supports homework and revision
- improves the presentation of their work
- connects learning at school with learning at home
- makes learning more fun.

All this can lead to better performance at school and an improved standard of work. For further information go to:

Parents Centre:
www.parentscentre.gov.uk/usingcomputersandtheinternet.
From the menu choose either **Links by topic** or **Links by age** for details of websites that will support children's learning.

APPENDIX 4 – Categories of Cyber bullying

Seven Categories of Cyber Bullying

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort.

- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.

- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.

- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.

- **Chat room bullying** involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.

- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online (i.e. MSN, Bebo, Facebook, Twitter, etc.).

- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber bullying.

- **Bullying via posts** is where people post nasty comments on another person's post on sites and apps such facebook, Instagram and youtube.

https://www.thinkuknow.co.uk/11_13/help/Contact-social-sites/

This site gives you a guide on how to report and remove unwanted posts or messages.

APPENDIX 5 – Advice for pupils regarding bullying

What can you do as a student?

If you are being bullied, remember bullying is never your fault. It can be stopped and it can usually be traced.

Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.

Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.

Text/Video Messaging

1. You can turn off incoming messages for a couple of days.
2. If bullying persists you can change your phone number (ask your Mobile Service Provider)
3. Do not reply to abusive or worrying text or video messages – your Mobile service provider will have a number for you to ring or text to report phone bullying.
4. Where possible save the messages.

E-mail

1. Never reply to unpleasant or unwanted e-mails
2. Don't accept e-mails or open files from people you do not know
3. Ask an adult to contact the sender's ISP by writing abuse and then the host e.g. abuse@hotmail.com.
4. Again save the email as evidence

Web

If the bullying is on the school website, tell a teacher or parent, just as you would if the bullying was face-to-face.

Chat Room and Instant Messaging

1. Never give out your name, address, phone number, school name or password online. It's a good idea to use a nickname. Do not give out photos of yourself either.
2. Do not accept emails or open files from people you do not know.
3. Remember it might not just be people your own age in a chat room.
4. Stick to public areas in chat rooms and get out if your feel uncomfortable.
5. Tell your parents or carers if your feel uncomfortable or worried about anything that happens in a chat room.
6. Think carefully about what you write – don't leave yourself open to bullying

ALWAYS TELL AN ADULT

APPENDIX 6 - Online safety further advice for schools

Key e-Safety Links for Schools

- ThinkUKnow - Resources for Teachers, Parents and Young People
- CEOP - Child Exploitation and Online Protection Centre
- Internet Watch Foundation
- UK Council for Child Internet Safety (UKCCIS)
- Childnet International

UK Safer Internet Centre