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 technology plays an important role in our everyday lives and we accept our responsibility to teach our staff and pupils how to use it 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 for 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 Online Safety 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 IT technician is responsible for reviewing the IT 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 IT technician 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 and 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 staff subsequently follow the school behaviour policy. J2E are able to monitor and close accounts if necessary.

Bullying

At Grand Avenue we deal with reported incidents of 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 Online Safety 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 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 Cyber Bullying from their professional association or union.

Victims of Virtual or Cyber bullying are advised to:

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

Prevention of Cyber Bullying

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

The subject of bullying (in all its forms) will be a regular topic for assemblies, themed weeks and circle times. The nationwide Safer Internet Day (usually taking place in February) is key to highlighting and addressing relevant issues faced by young people today.

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

Year	Concept	Skills	National Curriculum/content	Key Vocabulary
Year 1	Internet Safety	Know how to keep safe and how and where to get help	Begin to use technology safely and respectfully, keeping personal information private. Begin to identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies. *Core Theme 1 Unit 5 LESSON 6*	online bullying

Year	Concept	Skills	National Curriculum/content	Key Vocabulary
Year 2	Internet Safety	Recognise and respond to issues of safety relating to themselves and others and how to get help Recognise and manage risk in everyday activities	Use technology safely and respectfully, keeping personal information private. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies. *Core Theme 2 Unit 5 LESSON 7: Staying Safe – I Don't Know You*	online bullying, World Wide Web (WWW)

Year	Concept	Skills	National Curriculum/content	Key Vocabulary
Year 3	Internet Safety	Know how to keep safe and how and where to get help	Begin to use technology safely, respectfully and responsibly. Begin to recognise acceptable/unacceptable behaviour. *Core Theme 1 Unit 6 Lessons 1-4*	online bullying, World Wide Web (WWW)
		Recognise and respond to issues of safety relating to themselves and others and how to get help		

		Use strategies to stay safe when using ICT and the internet		
		Use ICT safely including using software features and settings		
		Behave safely and responsibly in different situations		

Year	Concept	Skills	National Curriculum/content	Key Vocabulary
Year 4	Internet Safety	Recognise and respond to issues of safety relating to themselves and others and how to get help	Use technology safely, respectfully and responsibly. Recognise acceptable/unacceptable behaviour. *Core Theme 1 Unit 6 LESSON 4: Online Privacy – It's Personal*	online bullying, World Wide Web (WWW), digital footprint, social network
		Use ICT safely including keeping electronic data secure		
		Begin to make responsible choices and consider consequences		
		Behave safely and responsibly in different situations		

Year	Concept	Skills	National Curriculum/content	Key Vocabulary
Year 5	Internet Safety	Know that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we	Begin to identify a range of ways to report concerns about content and contact.	online bullying, World Wide Web (WWW), digital footprint, social network, harassment,

		are anonymous Know how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met Know that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.	*Core Theme 2 Unit 4 LESSON 5: Online Relationships – A Risky Business*	blocking, junk mail

Year	**Concept**	**Skills**	**National Curriculum/content**	**Key Vocabulary**
Year 6	Internet Safety	To know how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted	Identify a range of ways to report concerns about content and contact. *Core Theme 1 Unit 5 LESSON 6: Internet Safety – Fake News*	online bullying, World Wide Web (WWW), digital footprint, social network, harassment, junk mail, in app purchasing, trolling, sexting, exclusion, doxxing, catfishing, flaming, fabotage, creeping, dissing, ghosting

Glossary:

catfishing	when someone steals your photos and uses them as their own, usually in a bid to meet other people on the internet or to trick or fool someone.
creeping	someone who follows someone else's social network profile closely.

cyber bullying	the use of electronic communication to bully someone.
digital footprint	a person's trail of data on the internet that can last indefinitely.
dissing	the act of commenting on a status with single liners that insult a specific person.
doxing	the publishing of an individual's home address or bank details etc.
exclusion	when an individual is passively ignored or actively rejected by others, and can occur face-to-face (offline) or via the Internet (online).
fabotage	accessing someone else's social media account without their knowledge and changing information on it.
flaming	the act of posting or sending offensive messages over the Internet. These messages, called "flames," may be posted within online discussion forums, or sent via instant messaging programs.
ghosting	breaking off a relationship by stopping all communication and contact without any apparent warning or justification.
harassment	the act of sending continuously offensive, rude and insulting messages.
in app purchasing	purchases of services or products possible within some apps, such as game apps, and real money is required by them.
junk mail	unwelcome or unwanted emails also known as spam.
sexting	sending and receiving sexually explicit images/videos via DM, text or social media.
social network	an online community where people can communicate and share information.
troll	a user who posts inflammatory messages typically on social media sites to upset others.
World Wide Web (WWW)	all of the web pages on the Internet, accessed using a browser.

APPENDIX 2 – Code of Conduct for Computing

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

See the Childnet 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. The 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. Step by step guides to follow are avaialable on how to make sure that children are as safe as they can be online.

Codes below can be scanned to get details on how to set parental controls on technology at home.

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 a guide on how to report and remove unwanted posts or messages.

APPENDIX 5 – Advice for pupils regarding bullying

Focus for teaching pupils strategies to use if being bullied.

Children are taught/reminded that ;

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