Grasmere Academy

Learn • Flourish • Achieve

Computing Policy

Includes Remote Learning Plan

Acceptable Use for Staff (Appendix 1)

Acceptable Use for Pupils (Appendix 2)

Date adopted by governors: May 2021

Committee: Ethos

Review date: May 2022

Statement of intent

Grasmere Academy believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. We understand the responsibility to educate our pupils on e- Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Both this policy and the Acceptable Use Policies (for all staff and pupils) include technologies provided by the school (such as iPads) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc).

1. Rationale

Pupils interact with the internet and other communications technologies such as iPads on a daily basis. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger. E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. Grasmere Academy takes these risks seriously and all emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

2. Aims

- To ensure all pupils and staff have a framework to work from with regards to e- safety.
- To protect the children in Grasmere Academy from potential harm.
- To educate children in the correct use of these technologies and how to report anything they deem as undesirable.
- To ensure the school has procedures for reporting and dealing with breaches to e-safety

3. Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-coordinator in our school is Miss Michelle Witty. It is the role of the e-Safety co-coordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health

and safety, home–school agreements, and behaviour/pupil discipline (including the antibullying) policy and PHSE.

4. Teaching and Learning

4.1 Why the Internet and emerging technologies are important.

- The Internet and many emerging technologies are an essential element to life in the 21st century. They are essential to education, business and social interaction. Our school has a duty to provide its pupils with quality Internet access as part of their learning experience and the ability to use new technologies for educational reasons.

- Internet use is a part of the statutory curriculum and a necessary tool for both pupils and teachers.

5. Managing Internet Access

5.1 Internet Access

- Pupils should not access the internet unless supervised.

- Staff will be allowed to use the internet for their own use as long as the access does not breach the e-safety policy.

5.2 Internet content

All internet content will be filtered by the North Tyneside filtering system.

- If staff or pupils do discover unsuitable material the e-safety coordinator should be notified. The URL should be noted and the site investigated. If the site is visited as an investigation the time and date of that access should be noted and the reason for accessing the site given.

- All unsuitable sites should be blocked due to the restrictions on the iPads, which is set up on new iPads as soon as they come into school. Any sites that are seen to be unsuitable that are accessed by pupils, should be documented on Cpoms under the E-safety link. The E-safety coordinator should then investigate into the restrictions to block the site.

5.3 E-mail

- All staff have a school email address provided through North Tyneside Learning Platform.

- Children will not be allowed access to the school email system without supervision.

- Teachers should be aware that their email accounts are not private and can be monitored.

- Children are not allowed to access any other web based email systems within school, for example, hotmail.

- Staff members may use personal web based email systems as long as it follows guidance in 4.1 of this policy.

5.4 Social networking and personal publishing

- Access to all social networking sites (networking sites such as facebook, my space, chat rooms, instant messaging, blogs, newsgroups) will be blocked using filtering systems.

- Pupils will be made aware that they should not publish any personal information on any website either in school or at home or arrange to meet anyone.

- The children should be made aware of how to report any behaviour they feel is inappropriate, i.e. report to parent or carer or to a teacher. This should include any online bullying.

- Parents should be made aware of the dangers of these sites and regular information meetings will be arranged by the school. These meetings will be run by Miss Witty.

5.5 School Website

- No contact details of pupils or staff will be included on the school website. Contact details will be the school address, email and telephone number.

- Only a child's first name will be used anywhere on the school website and in conjunction with any photographs used.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

6. Network Security and confidentiality

6.1 Network security

- School ICT systems capacity and security will be reviewed regularly.

- School iPads capacity and security will be monitored and reviewed regularly.

- The network operating system should be kept fully up to date with all appropriate updates and patches installed (this is the responsibility of the network manager).

- Teachers have an allocated laptop where possible. These are taken home. The use of these laptops at home must comply with the e-safety policy. When outside of school these laptops should only be used by the allocated teacher and no sensitive data should be stored on any laptop.

- No sensitive data should be stored on the hard drives of laptops.

- No sensitive data should be kept on memory sticks that do not have password protection.

- Teachers should not divulge their passwords to anyone except to the network manager or LEA staff for maintenance. If a password is divulged it should be changed immediately.

- It is good practise to change passwords every three months.

- Teachers should always lock workstations and laptops when left unattended.

6.2 Antivirus

The network has antivirus protection on the server and all workstations.

The virus definitions are kept up to date and a daily virus scan is scheduled. The virus checker also provides real time virus protection for internet access.

Digital images and video

School pictures and videos

- The school may use photographs and videos of the children for curriculum use without permission from parents/guardians.

- The school will seek permission from parents/guardians before photographs are used for display purposes, publication on the school web site or publication in local or national press.

- Any pictures or videos of children should be stored on the staff area of the school Google Drive. Once on the school Google Drive the images should be deleted from the camera.

6.3 Parental permission procedures

Parents/guardians will be given a photograph agreement form when their child first joins the school. This form will seek permission for:

- The use of photographs in displays.

- Permission for Seesaw use.

- The publication of photographs on the school website or in the press.

- Allowing other people associated with the school, for example, parents to photograph events involving their children.

This permission will be applicable for the duration of that child's time at Grasmere Academy.

The parents/guardians can change the agreement at any time by asking for a new permission form.

7. Mobile phones

7.1 Children's phones

- No use of mobile phones by children is permitted within school unless in an emergency and under supervision.

- All phones brought into school by pupils should be handed in at the office for secure storage. No phones should be kept in bags in corridors. This cuts down on risks of theft, texting, phoning, Bluetooth etc.

- Staff need to be aware of issues relating to phone bullying that can occur out of school.

- If children do feel they are suffering from phone bullying they should report this to their parents/carers or a teacher.

7.2 Staff phones

- Staff phones are permitted in school but should only be used for personal communication in non-teaching time when there are no children present.

- Staff should avoid taking pictures on a mobile phone. If an image is taken guidance in 6.1 of this policy should be followed.

8. E-safety complaints or non-compliance with policy

- All incidents of e-safety incidents or non-compliance to the policy should be recorded on Cpoms under the e-safety link.

- Any inappropriate websites visited by the staff or children should be logged with their URL for further investigation. If these sites are investigated the URL and date of the investigative visit should be logged.

- All incidents should be reported to the E-safety Co-ordinator and the head teacher.

- Inappropriate use of iPads will be dealt with according to the situation.

- Parents may be informed if the situation is deemed serious enough.

- Potential child protection or illegal incidents must be reported to the head teacher where appropriate steps will be taken.

9. How are stakeholders informed of this policy?

9.1 Staff

- This policy is written in consultation with the teaching staff. Staff are given a copy of the policy with time to discuss its implications to their teaching. The policy will also be stored on the school website.

- Staff will be educated in safe and acceptable use of social media.

9.2 Children

- Children will be given an acceptable use policy for e-safety. This policy will include the points relevant to children and will be in child friendly language. Children will be asked to write and sign this at the beginning of every year.

- Children will be educated in age relevant aspects of e-safety throughout the school.

9.3 Governors

- The draft policy is taken to the school governing body. The governors are given the opportunity to discuss the policy and its implications. This policy must be ratified by governors.

9.4 Parents

This policy will be available for parents to view via the school website.

Parents will be made aware of aspects relevant to them, for example, consent for images etc via letters from school.

The school will look at an evening meeting to inform parents of the dangers associated with e-safety.

10 Review of policy

- This policy will be reviewed annually in most cases.

- The policy may be reviewed in the light of incidents occurring in or out of school or with the emergence of new technology.

Remote Learning Plan

During the Covid-19 pandemic Grasmere Academy may expect some disruption to school routine by individual pupil, class or part school isolation.

School has considered the DFE guidance for home learning and has a strategy in place to facilitate home learning if and when the need arises.

Where a class, group or small number of pupils need to self-isolate, or there is a local lockdown requiring pupils to remain at home, we expect schools to have the capacity to offer immediate remote education. Schools are expected to consider how to continue to improve the quality of their existing offer and have a strong contingency plan in place for remote education provision by the end of September. This planning will be particularly important to support a scenario in which the logistical challenges of remote provision are greatest, for example where large numbers of pupils are required to remain at home.

In the schools contingency plan we have made the following arrangements:

Use a curriculum sequence that allows access to high-quality online and offline resources and teaching videos and that is linked to the school's curriculum expectations.

School will continue to offer learning based on the medium term and short term planning in place. Pre-recorded videos will be produced by staff in school and made accessible to affected pupils.

Give access to high quality remote learning resources

School has a Google Meet set up for all pupils in Years 1-Year 6.

All children have been issued with login details. School also has subscriptions to Oxford Owl, White Rose Maths, Sumdog, Times table Rockstars and Charanga to support with high quality resources.

If appropriate pupils may be directed to content from Oak Academy or BBC Bitesize also.

Parents can request a paper pack of resources if technology fails and they can't access online resources. iPads and internet dongles can be given to households who need them.

Select the online tools that will be consistently used across the school in order to allow interaction, assessment and feedback and make sure staff are trained in their use

School has a Google Meet set up for all pupils in Years 1-Year 6.

Staff have had experience during the initial school lockdown in Spring of using the virtual meeting system.

School also has class Twitter pages in operation to support as many of our parents engage using this method. The website has further information, including weekly timetables for remote learning. Seesaw is used to communicate with parents on a daily basis. Parents can contact teachers on Seesaw directly.

Recognise that younger pupils and some pupils with SEND may not be able to access remote education without adult support and so schools should work with families to deliver a broad and ambitious curriculum

Any pupils requiring bespoke provision will be supported by the class teacher and SENDCO. Physical resources will be considered and distributed as required.Teachers will provide parents with detailed individual targets to be worked on at home through Seesaw.

Set assignments so that pupils have meaningful and ambitious work each day in a number of different subject

Seesaw will provide learning that would have been covered in school across subjects. School will email this to parents if needed and can provide paper copies in the event that technology fails or can't be accessed. Tasks will be creative and practical were possible and will build on prior knowledge. School will also use White Rose Maths to support learning.

Provide frequent, clear explanations of new content, delivered by a teacher in the school or through high-quality curriculum resources or videos

Staff will offer pre-recorded sessions throughout each day via Seesaw.

Gauge how well pupils are progressing through the curriculum, using questions and other suitable tasks and set a clear expectation on how regularly teachers will check work

Teachers will communicate directly with parents via phone and through email to support and adjust learning based on parent feedback. Teachers will use Seesaw to access pupils' submitted work, to make assessments and give feedback.

Plan a programme that is of equivalent length to the core teaching pupils would receive in school, ideally including daily contact with teachers

Pupils are expected to complete three to four tasks from the home learning grid each day and upload their work by the end of the school day. These tasks should involve a maths, literacy, basic skills and project task. Parents should support the children wherever possible. Parents should set up a quiet work space for the child to have access to at home and should encourage the child to take regular breaks throughout the day. Parents should try to stick to a routine for starting and finishing the day as well as lunch times. This will be tailored around parents/carers, who need to work from home or at work as well, but it will be an expectation that all children will log on and access the work.

Appendix 1

Acceptable Use Policy
for the Internet and Electronic Mail by Grasmere Academy Staff

1. Introduction.

This document sets out the terms and conditions under which users will:

- Access the Internet
- Make use of resources / information on the Internet
- Disseminate information arising out of the Internet
- Disseminate information via the Internet
- Communicate using the Internet

This document applies to all staff, to whom the Internet is available via networked/ stand-alone computers and school laptops whether used at school or at home.

2. Purpose

The primary purpose of this document is to establish a set of rules and regulations to enable all users of the Internet to do so for the benefit of the school.

Additionally, this document aims to safeguard employees. Specifically to:

- Minimise (and where possible eliminate) the School's legal liability for the acts of employees using the Internet.
- Minimise (and where possible eliminate) the threat of damage to School property and or reputation by acts of employees using the Internet.
- Educate staff on their duties and obligations to the School and each other when using the Internet and the consequences of breaching them.
- Protect employees if this policy is breached by accident.

3. School Responsibilities

Implementing this Policy

The Headteacher and Board of Governors should implement this Policy in the way that best fits the working practices of the school. However, the implementation of this Policy should be carried out so that:

- Every user with Internet access is aware of it and understands its contents,

- Its regulations are enforced throughout the school,

- Breaches can be reported in a safe and confidential manner.

Under the authority of the Headteacher, the E-learning coordinator will ensure that staff usage of the Internet and electronic mail is carried out in accordance with this Policy. The E-learning coordinator should also have control over who in the school has access to the Internet. This Policy must also form part of the induction programme of all school employees who will have access to computers in the course of their work.

4. Warning against Deliberate Misuse of the Internet

The Internet is a valuable resource. It also presents significant dangers to the School from staff who may choose to abuse it. Whilst each case will be judged on its own merits, the following warning is issued to all staff:

(a). Any member of staff who commits a breach of any School Policy as a result of unauthorised use of the Internet (including electronic mail) will face disciplinary proceedings. Additionally:

(b). If the School discovers that a member of staff has committed a criminal offence or has been party to the commission of one as a result of unauthorised use of the Internet, the Police will be contacted immediately,

(c). The School will in no way indemnify a member of staff who has incurred any liability as a result of unauthorised use of the Internet. The School will seek financial redress from members of staff whose unauthorised use of the Internet causes the school suffer a loss.

5. Protection of staff acting in good faith

It is fully recognised that a member of staff may accidentally breach this Policy whilst acting in good faith and in the course of their duties as a member of staff of the School. If a member of staff suspects this to be the case, they MUST notify the Headteacher, E-learning coordinator IMMEDIATELY so that action can be taken to prevent or minimise damage and incidents can be logged on the school Cpoms system.

6. Authorised Uses of the Internet using school property whilst on school premises.

The school permits staff to use the Internet whilst in school in connection with school related matters only. This may include;

- The delivery of ICT lessons,

- Searching for lesson resources,

- Checking and responding to school emails using only school email logins, and

- Other school related searches on school appropriate search engine (Google Safe Search)

7. Unauthorised uses of the Internet

Whilst an act that does not fit the above categories will be considered an unauthorised use of the Internet, users attention is drawn to the following:

Strictly prohibited acts

The copying of software files from the internet should be kept to a minimum. No executable files should be copied from the internet and permissions for this on networked equipment is not granted.

- Do not access any sites or download or print any files displaying material that the user knows to contravene the School's Equal Opportunities Policy. If such a site is accessed inadvertently, either the Headteacher or E-learning Co-ordinator should be informed immediately.

- Do not access any site that involves any form of gambling or betting,

- Do not access any sites which provide a discussion or "chat" forum which does not fit the authorised uses listed above,

- Do not access free or personal email sites (e.g. Hotmail) in order to check private email whilst on school premises or when logged onto the school or admin accounts provided on staff laptops,

- Do not order any goods intended for school use via the Internet without consulting the Headteacher,

- Do not respond to surveys on the Internet on behalf of the School without consulting the Headteacher,

- Do not open a subscription account on the Internet on behalf of the School without express permission of the Headteacher,

- Do not allow anyone other than the named employee to use the Internet via the user's PC or school provided laptop.

- Do not use electronic mail for communication other than for purposes set out in Authorised Uses of the Internet, whilst on school premises or when logged onto the school account on a school laptop,

- Do not leave laptops in a state where it would be possible for someone other than the normal user (or other legitimate user) to access the Internet. Staff are responsible for logging off or locking a laptop when it is not in use,

- Do not leave your laptop or iPad unattended without locking it to your login or logging off,

- Do not let any other user access your ipad or laptop whilst you are logged on.

It is the responsibility of all users to report any unauthorised acts as soon as it comes to their attention to the E-learning co-ordinator or Headteacher of the breach who in turn should investigate the breach in consultation with the Council's ICT Services Manager.

Additionally, users are requested to follow the principles of good practice set out below:

Internet

- Do not reveal your own (or any other person's) personal details eg. home address, telephone number over the Internet,
- Connection time on the Internet must be of the shortest possible duration,
- Keep a record of sites which may be of use to your school and inform your E-learning coordinator of them so that they can be added to a list of suitable sites for other members of staff to refer to.

Electronic Mail

- Electronic mail should only be used in the course of your work as a school employee and only using the authorised logins provided by the school/ Platform.
- Electronic mail is not a person-to-person communication, always use appropriate language.
- Never use electronic mail to send or forward chain letters or any material which may contravene School policies.
- Inform the E-learning Co-ordinator if you know of anyone who should no longer be included in the school email address book.
- Keep messages as brief as possible and related only to work issues.
- Only copy messages (i.e. cc or bcc) to people where it is of direct relevance.
- If you are attaching documents, always ensure that the format is compatible with school equipment.
- At least once a week, ensure that all unwanted electronic mail messages are deleted from the Inbox, Sent and Deleted folders.
- Check your mailboxes regularly, at least once a day when in school.
- Ensure that messages arriving at your mailboxes are forwarded to another person if you are on leave for an extended period.

Social Networking Sites

As social networking sites are becoming increasingly popular in the digital world there has been a significant rise in the number of issues relating to social networking, particularly around Facebook. These incidents often include children, parents and on occasions teachers or governors having inappropriate discussions online in the mistaken belief that there comments are private. The fallout from such incidents is often serious and in some cases, has led to police action under harassment law. The views of a minority of individuals can influence and affect the larger community around a school. Incidents can

be personally challenging and time consuming for school leaders. Whilst social networking is usually filtered from school internet connections, many incidents relating to schools have taken place at home or whilst using mobile equipment. The following protocol must be followed in order to minimise, or where possible eliminate such incidents from arising;

- Guidance for security settings must adhered to and 'friends' with access to your social networking pages must be monitored closely.

- You should not accept or send friend requests to people whom you know through your professional role.

- You must not at any time post comments relating to the school, school community or indeed any other positions within the LEA that you have contact with through your professional role.

- You should be aware at all times that anything that you upload on to social networking sites could be viewed and thus potentially jeopardise your professional role.

8. Reviewing this Policy

This Policy will be officially reviewed annually as the use of the Internet in the school develops although it may be that the policy could be changed before this time due to developments within the curriculum, school or local council. If you have any comments about this Policy, please pass them on to the school E-learning co- ordinator or headteacher.

Appendix 2

Acceptable Use Policy for Pupils

The school has developed a set of rules to help keep pupils safe whilst using technology e.g. iPads, netbooks, Internet, email, Twitter, Blogging, Skype. Pupils will be reminded of their responsibilities whilst using technology. These rules will be kept under constant review and amended as required. Pupils MUST obtain the permission of their parent/guardian/carer before they can be allowed to use the internet/email system in school. The Parental Permission Form MUST be signed and returned to the school.

The following rules apply to ALL pupils:

- I will be responsible for my behaviour when using technology because I know these rules are to keep me safe.
- I will use school equipment & resources responsibly & with respect when directed by my teacher or member of staff. I will take full responsibility for damage caused to school equipment if used inappropriately.
- I will only use my own login and password that has been given to me by my teacher when using iPads/netbooks and online learning environments and will keep them secret.
- I will only use the internet in school for school work and follow my teachers or member of staff's instructions.
- I agree not to join or use any social networking sites other than authorised school Twitter class accounts (which are protected and monitored).
- I will turn off my device and tell my teacher or member of staff IMMEDIATELY if I see anything on the internet that makes me feel unhappy or uncomfortable.
- I will only send messages that are polite and sensible.
- I will turn off my monitor and tell my teacher or member of staff IMMEDIATELY if I receive an email that I don't like and will inform my parents if this happens at home.
- I will NEVER give out my own or others personal details e.g. name, address, phone number, etc.
- I will support the school approach to online safety and NOT deliberately download/upload any images, videos, sounds or text that could upset any member of the school community.
- I know that the school can check my files and internet sites that I visit will be filtered and monitored. The school may contact my parent/guardian/carer if the school is concerned about my E-Safety.
- I will NOT bring data storage devices (USB sticks, memory cards, etc) into school without permission from my teacher or member of staff and where possible will upload such documents to the Platform.
- I will NOT bring my mobile phone into school without my parent's knowledge.
- I will never use ICT in an offensive way that may hurt or upset others.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement when I am outside of school and where they involve my membership of the school community (examples would be Cyberbullying, use of images or personal information).

SANCTIONS

1. A letter home informing parent/guardian/carer of the nature and the breach of rules.
2. Local Authority informed.