Grange Park Prep School

Online Safety Policy and Guidelines

Document created by:	Flavia Rizzo (Headteacher) January 2017
Reviewed by:	Flavia Rizzo 13th September 2021
Next review date:	September 2022

INTRODUCTION AND PRINCIPLES

Technology has transformed the process of teaching and learning inside schools. It is a crucial component of every academic subject and is also taught as a subject in its own right. All of the school's classrooms are equipped with interactive projectors/apple TV and computers. All our pupils are taught how to research on the internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution. Technology also plays an enormously important part in the lives of all young people outside schools. Sophisticated games consoles, like XBox, Playstation, Wiis and Nintendo DS, together with internet enabled mobile phones and smartphones provide unlimited access to the internet, to SMS messages, to blogging (web logging), to social media websites (like Twitter), to Skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms and other social networking sites (such as Facebook), and video sharing sites (such as YouTube). This communications revolution gives young people unrivalled opportunities. It also brings risks. The School takes every step necessary to ensure that all the pupils in its care are safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

SPECIFIC OBJECTIVES

1. To set out within the field of technology the areas of concern and action on the part of the School.
2. To indicate who is affected by this policy and when.
3. To set out the roles and responsibilities of the School and its staff; and of parents or guardians
4. To emphasise the importance of staff awareness and training
5. To identify how the School emphasises the importance of the curriculum in making sure that there is a full understanding of the issues and of how the whole community can be involved in ensuring safety
6. To indicate our policies on personal devices of staff and children
7. To indicate our policies on the use of the internet, emails and texts
8. To set out how we teach staff and pupils to ensure their own safety and that of others by using password security, and ensuring safe data storage and appropriate use of images
9. To ensure that children are safe from terrorist and extremist material that promote radicalisation when accessing the internet in school, by establishing appropriate levels of filtering and monitoring.[1]
10. To indicate how parents can make a complaint in the event of dissatisfaction arising out of a process or event.

[1] Prevent Duty Guidance for England and Wales, 2015

AREAS OF CONCERN

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used both in and outside of School may include:

- Websites;
- Email and instant messaging;
- Blogs;
- Music / video downloads;
- Text messaging and picture messaging;
- Video calls;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

WHO THIS POLICY IS INTENDED TO COVER, AND WHEN ?

This policy is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. Whilst exciting and beneficial, both inside and outside of the context of education, many online resources are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

We understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

This policy covers both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices which might be owned by pupils and staff and brought onto School premises (personal laptops, tablets, smart phones, etc.).

ROLES AND RESPONSIBILITIES

ROLE OF OUR STAFF

With the expansion in technology, the school recognises that blocking and barring sites is no longer adequate. The School teaches all of its pupils to understand why they need to behave responsibly if they are to protect themselves. The school's technical support have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and web filtering and for training the school's teaching and administrative staff in the use of ICT.

ROLE OF OUR DESIGNATED SAFEGUARDING LEAD

The School recognises that online safety is a safeguarding issue. The Designated Safeguarding Lead (DSL) Flavia Rizzo and the Deputy DSL Helen Billam and EYFS DSL Dimitra Louskas have responsibility for ensuring this policy is upheld by all members of the School community. They keep up to date on current online safety issues and guidance issued by organisations such as the CEOP (Child Exploitation and Online Protection) a national Police Agency, whose hyperlink is: http://ceop.police.uk/, Childnet International and the Local Safeguarding Children Board (LSCB) and NSPCC. As with all issues of safety at this School, staffs are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

ROLE OF PARENTS

The School believes that it is essential for parents to be fully involved with promoting online safety both in and outside of School. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

STAFF AWARENESS AND TRAINING

All new teaching staff receive information on the School's suite of Safeguarding policies as part of their induction. All teaching staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All specialist staff also receive our Online Safety Policy on arrival at School. Agency staff providing short-term cover (which may only be provided for a day or part of a day will be requested to peruse a summary sheet of information and to refer to the DSL for all guidance). Where such cover extends beyond a week the agency staff member will be expected to fulfil all the requirements expected of staff in permanent employment.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School online safety procedures. When children use School computers, staffs make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community. A record of concern must be completed by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the School's DSL.

ONLINE SAFETY IN THE CURRICULUM AND SCHOOL COMMUNITY

IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be

encountered outside School will also be carried out via PSHE, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught to look after their own online safety. Pupils are informally taught about recognising online exploitation of any kind and of their duty to report any such instances which they, or their peers, come across. Pupils can report concerns to the DSL and any other member of staff at the School.

The Children in KS2 are asked to sign the school ‘online safety agreements’ parents are also shown this and asked to sign that they understand the agreement, younger children are asked to have these signed by parents on behalf of the children.

Pupils are taught about respecting other people's information and images (etc.) through PSHCE sessions.

Pupils should be aware of the impact of cyber-bullying (see also the School's Anti-bullying Policy) and the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people. Pupils should know how to seek help if they are affected by these issues. Pupils should approach the DSL as well as parents/guardians, peers and other School staff for advice or help if they experience problems when using the internet and related technologies.

The School utilises Microsoft Family Safety to provide a web filtering service.

MISUSE: STATEMENT OF POLICY

The school will not tolerate the accessing of inappropriate or illegal material and will always report illegal activity to the police and also the LSCB if appropriate. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP) in addition to the LSCB. The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying policy.

PERMITTED USE OF SCHOOL AND PERSONAL DEVICES

STAFF

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Staff are permitted to bring in personal devices for their own use but are not allowed to have their phone switched on during the working day. They may use their mobile telephone only during break-times and lunchtimes. Personal telephone numbers may not be shared with pupils or parents and under no circumstances may staff contact a pupil or parent using a personal telephone number.

PUPILS

Mobile technologies available for pupil use [including laptops, tablets, etc.] are stored a locked cupboard, with access only available via the class teacher. No personal devices belonging to pupils are to be used during lessons at School. If pupils bring in mobile phones [(e.g. for safety purposes if they walk to and from School alone)], they must be handed in to

the Administrator's office at the start of the day and collected as they leave School. (Covid Changes: See Appendix 1)

USE OF INTERNET EMAIL AND DEVICES, INSIDE AND OUTSIDE OF SCHOOL

STAFF

Staff may not access any social networking or other websites or personal email which is unconnected with School work or business either from School devices or whilst in front of pupils. Such access may only be made from their own personal devices whilst in staff-only areas of School.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications may be monitored.

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

Any online communications will neither knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting links or material which is discriminatory or offensive.

Any digital communication between staff and pupils or parents is expected to be professional in tone and content. Under no circumstances may staff contact a pupil or parent using any personal email address.

PUPILS - CHARTER FOR SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT THE SCHOOL

Online safety is a whole school responsibility and the staff have adopted a charter with pupils for the safe use of the internet inside the school with the following elements:

1. CYBERBULLYING

● Cyberbullying, defined as bullying through the use of electronic devices, is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can 7 be no safe haven for the victim, who can be targeted at any time or place. The school's anti-bullying policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.

● Proper supervision of pupils plays an important part in creating a safe ICT environment at school but everyone also learns how to stay safe outside the school.

● The School values all of its pupils equally. It is part of the ethos of the school to promote considerate behaviour and to value diversity.

● Bullying and harassment in any form, including being targeted or influenced to participate in radicalism or extremism, should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

2. TREATING OTHER USERS WITH RESPECT

● The school expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the school's Behaviour Policy (copies of which are sent to parents).

● The school expects a degree of formality in communications between staff and pupils. They should not communicate with each other by text or mobile phones.

● Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school's anti-bullying policy is set out on the school website. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.

● All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of the pastoral staff.

● The use of mobile phones within school hours is not allowed in school premises. Pupils who need to have access to a mobile phone out of school hours are instructed to deliver their mobile phone to the School Administrator at the start of the school day and to collect it as they leave school. The use of this mobile phone will not be allowed on school premises, or otherwise until such time as the pupil and mobile have been handed over to their parents' designated responsible adult.

3. KEEPING THE SCHOOL NETWORK SAFE

● The school adheres to best practice regarding e-teaching and the internet.

● Certain sites are blocked by the school's filtering system and the school's IT department is able to monitors pupils' use of the network.

● The IT department monitors email traffic and blocks SPAM and certain attachments.

● The school has anti-virus protection on its network which is administered by the school's IT support.

● Any member of staff or pupil who wishes to connect a removable device to the school's network is asked to arrange in advance with their class teacher who will ensure the appropriate clearances

There is strong anti-virus and firewall protection on our network and certain websites are automatically blocked by the School's filtering system; in addition, spam emails and certain

attachments will be blocked automatically by the email system. If these issues cause problems for School work or research purposes, pupils will speak to their classroom teacher for assistance.

Pupils should immediately report, to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils must report any accidental access to materials of an inappropriate nature [e.g. if violent or sexual] directly to the DSL. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the School's Behaviour Policy. Pupils are aware that all internet usage via the School's systems may be monitored.

The School expects all pupils to adhere to this policy for the safe use of the internet.

To ensure that there are no incidents of misuse, or attempted misuse of the internet, personal mobile phones and other electronic devices are not permitted to be used to access the school's ICT facilities.

DATA STORAGE

The School takes its compliance with the Data Protection Act 1998 seriously.

Staff and pupils are expected to save all data relating to their work to the School's central server or Google Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. The School expects all removable media (USB memory sticks, CDs, portable drives) taken outside School or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by School.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the class teacher.

PASSWORD SECURITY

Pupils and staff have individual School network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security. All pupils and members of staff are expected to:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed as a minimum every school year;

- not write passwords down; and

- not share passwords with other pupils or staff.

SAFE USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at School events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images may not be published on blogs or social networking sites (etc.), nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment: personal equipment should not be used for such purposes.

Care is taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute. Pupils may not take, use, share, publish or distribute images of others without their permission.

Written permission from parents will be obtained before photographs of pupils are published on the School website or elsewhere.

Photographs published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

COMPLAINTS

As with all issues of safety at the School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the class teacher in the first instance, who will undertake an immediate investigation and liaise with Head and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Incidents of or concerns around online safety will be recorded using an Incident Report form and reported to the School's DSL in accordance with the School's Child Protection Policy. This policy will be reviewed in September 2021.

Appendix 1:

Due to the current Covid-19 guidelines on maintaining social distance and not sharing resources, the children are permitted to use their own devices for the purposes of accessing their learning during lessons only. Children are monitored and have been trained to only use the application or website that the class teacher has allocated for the lesson. Devices are kept securely in the children's desk and are only permitted under the supervision of the member of staff teaching them. Children and parents have also signed a 'Responsible User Agreement'.