Online Safety Policy

ABSTRACT
How we, as an organisation, ensure the safety and wellbeing of pupils and staff with regards to online devices

APPOVED	Headteacher
POLICY DATE	Autumn 2022
REVIEW	Autumn 2023

Online Safety Policy

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms –Google classroom
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Aims and objectives:

- To ensure the safety and wellbeing of children and young people when adults, young people or children are using the internet, social media or mobile devices
- To provide staff and volunteers with the overarching principles that guide our approach to online safety
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

We believe that:

- Children and young people should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however it can also present risks and challenges
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep children and young people safe online, whether or not they are using [name of organisation]'s network and devices
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- appointing Computing Lead - tbc
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Guidelines

1. **Pupils' online access**

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Responsible usage of the Internet for all pupils should be taught routinely through Computing. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "What is the

purpose?"

Children will be taught use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Sharing websites via J2e and Google are a useful way to present this choice to pupils.

2. **Filters**

Grange Primary School has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network. We use the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, and prevents access to extremist websites and materials etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status. We use user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students. Our SBT (school based technician) ensures the network is healthy through use of anti-virus software (from LGfL) etc and the network is set up so staff and pupils cannot download executable files. All chat rooms and social networking sites are blocked except those that are part of an educational network or approved Learning Platform. Any sites which the school wants unblocking needs authorising through the head teacher, and a written request needs to be raised on the Adept Support website which will be processed by a member of the RM Remote Support team.

3. **Online Safety**

All teachers are responsible for promoting and supporting safe behaviour in their classroom and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture where pupils feel able to report any bullying, abuse or inappropriate materials. Children will receive Online-Safety education once an academic year, to teach them the importance of being safe online and highlighting the potential dangers that they can be exposed to.

Online safety is taught in every year group.

Social Networking Sites - These are a popular aspect online for young people. Sites such as: Facebook, Instagram, Snapchat, WhatsApp, YouTube and TikTok allow users to share information and communicate with each other. It is important for children to understand that most social networking sites carry an age restriction of 13 and that this space is used by the vast majority of the population; these are environments that should be used with caution.

Prevent Duty

As a school we aim to ensure that children are safe from terrorist and extremist material when accessing online at school. As outlined above, suitable filtering is in place to protect pupils. All teachers are aware of the risks posed by the online activity of extremist and terrorist groups, and by communication with parents and sharing guidance on safe internet access at home and supervision by an adult, we aim to ensure that pupils are protected from the threat of radicalisation. In the case of any member of staff or pupil attempting to access inappropriate material online, the school would make a referral to the Channel programme in accordance with government and Local Authority guidelines, See the school's Prevent Duty Document.

Pupils:

We use J2e and Google with the pupils and lock this down where appropriate using LGfL filtering. Pupils' USO and Google accounts are not visible to others and handed out to that person only. Pupils are introduced to the cloud and working collaboratively on a document and communicating online as part of the Computing scheme of work. Pupils are taught about the safety of communicating online both in school and at home i.e. they are taught:

- not to give out their username and password unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- they must not reveal private details of themselves or others in an online, such as an address, telephone number, etc;
- to 'Stop and Think Before They Click' and not to open a link unless they are sure the source is safe;
- that they should think carefully before uploading any attachments as this will remain online forever;
- that they must immediately tell a teacher / responsible adult if they receive a document online which makes them feel uncomfortable, is offensive or of a bullying nature;
- not to respond to malicious or threatening messages.

4. **Use of email**

We do not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@grange for communication with the wider public. The school will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law. The school manages accounts effectively with up to date account details of users. We are aware that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

5. **Web publishing**

The school has its own website, and the school is registered with the ICO under the Data Protection Act. Parental consent is gained upon admission to the school. This is required before

any text, audio, pictorial or photographic reference to a child or children being published. Records are kept of parents or carers who decline permission. Individual pupils will not be identifiable by name, and names will not be linked to any photographs. Personal information will never be published without prior consent.

6. **Reporting incidents**

If one or more pupils discover (view) inappropriate material, the first priority is to provide them with support. Children should report any unsuitable sites to the class teacher. The class teacher is then responsible to report the inappropriate material to the Safeguarding Lead. From there the Computing coordinator should inform the head teacher.to the upgraded LGFL filters there are a lot more restrictions placed upon the internet.

Incidents which occur due to non-compliance with the school Online Safety policy and issues relating to staff misuse must be referred to the head teacher. Any incidents which refer to children protection must be reported to the Designated Safeguarding Lead.

7. **Parents and the community**

Pupils' online access at home is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy. Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website.

8. **Roles and responsibilities**

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the senior management team.

Our school Online Safety Co-ordinator is Ms Charles.

Our Online Safety Co-ordinator ensures that they are up to date with Online Safety issues and guidance through the Local Authority Online Safety Officer and through organizations such as Becta, LGFL, NSPCC and CEOP. The school's Online Safety Co-ordinator ensures the Head, senior management and the Governors are updated as necessary.

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- The Education Space are our appointed Data Protection Officer (DPO), with responsibility for data protection compliance.

- We have listed the information and information asset owners in our Information Asset Register.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record.

  We ensure ALL staff are sent an Acceptable Use Agreement (updated September 2022) and keep a register of signatures to confirm that this has been received and read.

  This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks. We monitor school e-mails / online platforms, etc. to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- Relevant Admin / SLT staff access confidential school information via the MyUSO portal which uses 2 factor authentication.
- School staff who set up usernames and passwords for e-mail, network access, or other online services work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.
- Any new technologies which require the sharing of personal data first are subject to a DPIA (Data Processing Impact Assessment) by our Data Protection Officer to assess the level of risk. Any companies, apps or websites that we use have fully transparent Data Protection Policies. We keep the sharing of personal data to a minimum outside of what is required by the DfE, Newham etc. This is outlined in our Privacy Notice and Data Policy.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the Pan-London Admissions system to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use LGfL AutoUpdate for creation of online user accounts for access to services and online resources.

- We use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.
- We store any sensitive/special category written material in lockable storage cabinets in a locked room
- All servers are in lockable locations and managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our network / admin, curriculum server(s).
- For ICT disposal, we delete all data from hard drives and memory and dispose of the equipment via Newham Council
- Portable equipment loaned by the school for use by staff at home, where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded.
- Visitor log ons have restricted access to curriculum drives.

Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. As part of the LGFL filtering these sites are blocked within school, however as a duty of care to both students and adults it is our responsibility to educate about the potential dangers.

Information and support:
There is a wealth of information available to support schools and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	What it does/provides
Think u Know	NCA CEOPs advice on online safety
Disrespect Nobody	Home Office advice on healthy relationships, including sexting ar pornography
Parent Zone	Help for parents on how to keep their children safe online
Childnet.cyberbullying	Guidance for schools on cyberbullying
Educate Against Hate	Practical advice for parents, teachers and governors on protectir children from extremism and radicalisation.
UKCIS	The UK Council for Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
NSPCC	NSPCC advice for parents
Common sense Media	Independent reviews, age ratings, & other information about all types of media for children and their parents
Searching, Screening and Confiscatio	Guidance to schools on searching children in schools and confiscating items such as mobile phones
LGFL	Advice and resources from the London Grid for Learning

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding, Early Help & Child Protection policy
- Behaviour Policy
- Whistleblowing Policy
- Staff Handbook
- Data Policy