inspirans flammas
posteritatis

ROSEMEAD
PREPARATORY
SCHOOL & NURSERY
DULWICH

P14.3 - ONLINE SAFETY POLICY

(INCLUDING EYFS)

Reviewed: Michaelmas 2022
Next review: Michaelmas 2023

BACKGROUND AND AIMS

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

But as the school increasingly works online, it is essential that our children are safeguarded from potentially harmful and inappropriate online material. As such, we will ensure that appropriate filters and appropriate monitoring systems are in place.

The use of these new technologies can put young people at risk within and outside the school. Technology can often provide the platform to facilitate harm: child exploitation, radicalisation, sexual predation. We aim to establish mechanisms to identify, intervene in, and escalate any incident where appropriate.

Many of these risks reflect situations in the off-line world and it is essential that an effective online safety policy and approach is used in conjunction with other school policies.

RELATED POLICIES

Positive Behaviour Policy

Anti-bullying Policy

Child protection policies including Prevent

Computing and Digital Learning Policy

Personal Portable Device Policy

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

GOVERNORS

The Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy which is undertaken by the Health and Safety Committee who then report to the full Board.

THE SLT (See ANNEX 1)

The SLT is responsible for ensuring the safety (including online safety) of members of the school community. Every SLT meeting will include online safety under the 'health and safety' agenda item.

The SLT is responsible for ensuring that the online safety Officers and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The SLT will receive regular updates from the online safety Officers.

The SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

ONLINE SAFETY OFFICERS (See ANNEX 1)

The Computing Co-ordinators perform the role of Online Safety Officers and discuss any online safety issues with the Headmaster who in turn would bring them to the attention of the Health and Safety Committee.

THE NETWORK MANAGER (See ANNEX 1)

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- that the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that the use of the network/Virtual Learning Environment (VLE)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the SLT for investigation/action/sanction.

TEACHING AND SUPPORT STAFF

Teaching and support staff must read the 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' document.

This guidance document, commissioned by the Department for Education (DfE), provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. It has specific sections that relate to photography, video, and internet usage.

It aims to:

- keep children safe by clarifying which behaviours constitute safe practice and which should be avoided.

- assist adults working with children to do so safely and responsibly, and to monitor their own standards and practice.
- support managers and employers in setting clear expectations of behaviour and codes of practice.
- support employers in giving a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- support safer recruitment practice.
- minimise the risk of misplaced or malicious allegations made against adults who work with children.
- reduce the incidence of positions of trust being abused or misused.

Teachers and support staff must be aware of the potential use of social media for on-line radicalisation; the latest resources can be found from the DfE's "How Social Media is used to encourage travel to Syria and Iraq, Briefing Note for Schools"

In addition, teaching and support staff must read the school Acceptable Use Agreement for Staff and Volunteers. (See ANNEX 2)

CHILDREN

All Pre-prep children must be made aware of the importance of online safety by their teachers and parents. Their parents must read the Acceptable Use Agreement for Pre-prep Children and Parents contained within their Reading Diaries on their behalf. (See ANNEX 3)

All Prep children must read the Acceptable Use Agreement for Prep Children and Parents contained with their Homework Planners. (See ANNEX 4)

We give the children online safety sessions annually to aid their understanding of the issues. The document 'Teaching online safety in school', from the DfE, outlines how schools can ensure their pupils understand how to stay safe and behave online.

PARENTS

All parents must read the Acceptable Use Agreement relating to their child's age group and ensure that their children understand and adhere to it. (See ANNEX 3 and 4). We also offer online safety workshops to parents to aid their understanding of the issues.

POLICY STATEMENTS

EDUCATION - CHILDREN

Online safety education will be provided in the following ways:

- As part of a broad and balanced curriculum through teacher led lessons as well as professional workshops. Resilience to protect themselves and their peers is also taught and information provided.
- Relevant issues regarding safeguarding and online safety may be covered in Relationships Education.
- Rules for use of ICT systems/internet will be displayed on log-on screens
- Staff should act as good role models in their use of ICT
- Resources that are available to support the teaching of online safety can be found in Annex 5.

EDUCATION AT HOME

Where children are being asked to learn online at home, there is advice to do so safely in these documents: 'Safeguarding in schools, colleges and other providers' and 'Safeguarding and remote education.'

EDUCATION AND TRAINING - STAFF

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online-safety training will be made available to staff. The needs of online safety training for staff will be reviewed regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use policies.

TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Health and Safety Committee.
- All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Head or other nominated senior leader and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school has a managed filtering service. Any usage that is flagged as a safeguarding concern is shared with SLT and appropriately dealt with. The monitoring of websites visited and blocked is also shared.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Head.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school laptops and other portable devices that may be used out of school, see Acceptable Use Agreement.
- The school infrastructure and individual workstations are protected by up to date anti-virus software.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Use encryption and secure password protection when transferring data to other schools and outside agencies

RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In such cases:

- A child can report the incident to a teacher (or to the Head)
- A teacher can report the incident to his or her line manager
- A parent can report the incident to the form teacher or member of the SLT
- The Head can report the incident to the Chair of Governors

These incidents of misuse are managed through the Positive Behaviour, Anti-Bullying or Safeguarding policies and procedures. An escalation in incidents would involve more serious sanctions being put in place.

ANNEX 1 – POST HOLDERS

Role	Post Holders
SLT	Phil Soutar
	Lisa Meredith-Bennett
	Lesley Kastoryano
	Ray Sawyer
	Graeme McCafferty
Online Safety Officers	Romilly White Amity MacDonnell

Network Manager	Andrew Soong

ANNEX 2 - ACCEPTABLE USE AGREEMENT FORM FOR STAFF AND VOLUNTEERS

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, the Drive etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school below.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website, it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (tablets/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any intentional damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

ANNEX 3 - ACCEPTABLE USE AGREEMENT FORM FOR PRE-PREP CHILDREN AND PARENTS

I understand that my child must use school ICT systems in a responsible way, and that I must ensure that they understand the importance of online safety.

I understand that the security of personal data sent to me by the school is my responsibility.

I have told my child that:

- The school will monitor his/her use of the ICT systems.
- He/she should tell the teacher if he/she sees something on-line that makes them uncomfortable.
- He/she should only use the computer programmes that the teacher tells him/her to use.
- He/she should not take or use another child's work without their permission.
- He/she should tell the teacher immediately if equipment gets damaged.
- He/she should be safe online at home as well as school.

ANNEX 4 - ACCEPTABLE USE AGREEMENT FORM FOR PREP CHILDREN AND PARENTS

As a child:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety, I understand that:

- The school will monitor my use of the ICT systems, email and other digital communications within the school systems.
- I will not share my password, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when on-line.
- I will tell my teacher immediately if I see something on-line that makes me feel uncomfortable.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not meet unknown people off-line that I have communicated with on-line without an adult with me and only in a public place.

I understand that everyone has equal rights to use technology as a resource and:

- I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try to make large downloads or uploads unless I have permission to do so.

I will act as I expect others to act toward me:

- I will not take or use another child's work without their permission.
- I will not take or distribute images of anyone without their permission.

I understand that the school needs to keep its ICT safe and running smoothly:

- I will only use my own ICT equipment in school if I have permission.
- I will only use the computer programmes that the teacher tells me to use.
- I will tell the teacher immediately if equipment gets damaged.
- I will not open an email attachment unless I know and trust the person who sent it to me.

When using the internet for research or recreation:

- I will make sure I have permission to use any downloaded material that is not mine.

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

- I will be safe online at home as well as school.

I understand that if I do not follow these guidelines, there will be an appropriate sanction.

As a parent:

I understand that my child must use school ICT systems in a responsible way, and that I must ensure that they understand the importance of online safety and adhere to the above. I also understand that I have a responsibility to ensure that a similar level of online safety is provided at home. I understand that the security of personal data sent to me by the school is my responsibility.

ANNEX 5 - RESOURCES FOR SUPPORT IN TEACHING ONLINE SAFETY

- **Be Internet Legends** developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- **Disrespectnobody** is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- **Education for a connected world framework** from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- **PSHE association** provides guidance to schools on developing their PSHE curriculum
- **Teaching online safety in school** is DfE guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- **Thinkuknow** is the National Crime Agency/CEOPs education programme with age specific resources
- **UK Safer Internet Centre** developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.
- **Harmful online challenges and online hoaxes** this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support