

E-safety Policy 2016



Policy agreed: September 2016

Review date:

Nexus Education Schools Trust (NEST)

group of schools

Contents:

Page 3	Schedule for Development/Monitoring/Review
Page 3	Scope of the Policy
Page 3	Roles and Responsibilities:
Page 3	Governors
Page 4	Headteacher and Senior Leaders
Page 4	E-Safety Coordinator/Designated Senior Person
Page 4	Network Manager
Page 5	Teaching and Support Staff
Page 5	Child Protection/Safeguarding Designated Person
Page 6	Students
Page 6	Parents/Carers:
Page 6	Community Users:
Page 7	Policy Statements
Page 7	Education – students
Page 7	Education – parents/carers
Page 8	Education – The Wider Community
Page 8	Education & Training – Staff/Volunteers
Page 8	Training – Governors
Page 8	Technical – infrastructure/equipment, filtering and monitoring
Page 9	Bring Your Own Device (BYOD)
Page 10	Use of digital and video images
Page 10	Data Protection
Page 11	Communications
Page 11	Social Media - Protecting Professional Identity
Page 12	Appropriate and Inappropriate Use by Staff or Adults:
Page 12	In the Event of Inappropriate Use
Page 12	Appropriate and Inappropriate Use by Children or Young People:
Page 13	In the Event of Inappropriate Use
Page 13	Responding to incidents of misuse
Page 14	Illegal Incidents
Page 15	Other Incidents
Page 16	APPENDIX 1 - Secure transfer of data and access out of school
Page 17	APPENDIX 2 - ACCEPTABLE USE AGREEMENT (Staff/Volunteer

E-Safety policy

E-safety encompasses internet technologies and electronic communications such as mobile phones, iPads, Laptops and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including safeguarding and behaviour.

The school has appointed an e-safety designated senior person.

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body: June 2016. Monitoring of the E-Safety Policy will take place at regular intervals. The Governing Body will receive a report on the implementation of the E-Safety Policy. The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be June 2017. The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of:
 - students
 - parents/carers
 - staff

Scope of the Policy

This policy applies to all members of Farnborough Primary School (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Farnborough School ICT systems, both in and out of the School.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Farnborough School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Farnborough Primary School.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator/Designated Senior Person
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

Headteacher Heads of School and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety designated Senior Person.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher/Senior Leadership Team are responsible for ensuring that the E-Safety designated Senior Person and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety designated Senior Person.

E-Safety Designated Senior Person:

- leads on e-safety issues
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack. that the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply. that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ E-Safety designated Senior Leader for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement .
- they report any suspected misuse or problem to the Headteacher/E-Safety designated Senior Person for investigation/action/sanction.
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the e-safety and acceptable use agreements.

- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
 - they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
 - in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Child Protection/Safeguarding Designated Person:

The Child Protection/Safeguarding Designated Person

should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website.
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff will reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of ICT/PSHCE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

- Staff should act as good role models in their use of digital technologies the internet and mobile devices
 - in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
 - Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
 - It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents/carers:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents/Carers evenings
- High profile events/campaigns eg Safer Internet Day

Education & Training – Staff/Volunteers:

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors:

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in the following way:

- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

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:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The school has provided enhanced/differentiated user-level filtering
- The network manager regularly monitors and records the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.

- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
 - CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
 - USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
 - Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

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/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will 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 eg on social networking sites.
 - In accordance with guidance from the Information Commissioner’s Office, parents/carers 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 should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
 - Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; where the staff uses personal equipment any images will be transferred to school devices and deleted from staff devices as soon as possible.
- Care should be 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 must not take, use, share, publish or distribute images of others without their permission.
 - Photographs published on the website, or 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.
 - Written permission from parents or carers is obtained before photographs of pupils are published on the school website.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.

Staff must ensure that they:

11

- 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.
- Transfer data using encryption and secure password protected devices.

Signed: Chair of Governors

Signed: Governor with responsibility for Inclusion or Equality

Signed: Headteacher

Date: