‘Learn to live, live to learn’

Foxyards Primary School

E-Safety Policy

Drafted by: Mrs Helen Thomas, Headteacher September 2018	Approved by:
Date to be reviewed: September 2019	

Roles and Responsibilities

Head teacher and Senior Leaders:

The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community and is likely to be the school's Senior Information Risk Owner (SIRO) The schools SIRO is responsible for reporting security incidents as outlined in the schools Information Security Policy. The day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator who has this responsibility.

The Head teacher /SLT are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately

The Head teacher / SLT 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 SLT will receive regular monitoring reports from the E-Safety Co-ordinator / Officer

The Head teacher and another member of the SLT 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.

The Head teacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via an online communication system, have adequate information and guidance relating to the safe and appropriate use of this on line facility.

The Head teacher or a designated member of the SLT is responsible for ensuring that parents/carers understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures and as stipulated in the Social Media Policy.

E-Safety Coordinator / Officer:

The school has a named person with the day to day responsibilities for E-Safety.
Responsibilities include:
Taking day to day responsibility for E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies / documents
Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place

Providing training and advice for staff
Liaising with the Local Authority, DO (LADO) or relevant organisations
Liaising with the schools SIRO to ensure all school data and information is kept safe and secure
Liaising with school ICT technical staff and/or school contact from the managed service provider- RM Unify.
Receiving reports of E-Safety incidents and creating a log of incidents to inform future E-Safety developments
Meeting regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering
Attending relevant meetings / Governor committee meetings
Reporting regularly to the Senior Leadership Team

Managed service provider (applicable to DGfL3 schools):

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by DGfL. The managed service provides a number of tools to schools including Securus, Smoothwall filtering and MDMs (Mobile Device Management systems), which are designed to help schools keep users safe).
Schools are able to configure many of these locally or can choose to keep standard settings.
A designated adult can access activity logs for network users and apply 'rules' to specific group of users.
The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Policies/guidance and include relevant Local Authority E-Safety policies and guidance.
http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/safeguarding-children-procedures/
http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/e-safety-and-use-of-images/
Members of the DGfL team will support schools to improve their E-Safety strategy
The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the DGfL team.

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 encourage pupils to develop good habits when using ICT to keep themselves safe
They have read, understood and signed the school Staff Acceptable Use Policy (AUP/AUA)
They report any suspected misuse or problem to the E-Safety Co-ordinator or SLT
Digital communications with students / pupils (email / Virtual Learning Environment (VLE)applications/O365 Apps/Google Apps / voice) 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 school activities
Students / pupils understand and follow the school E-Safety and acceptable use policy
Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
They monitor ICT activity in lessons, extra-curricular and extended school activities
They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices, including their personally owned devices and that they monitor their use and implement current school policies with regard to the use of these devices in school or during extended school activities.
In lessons, where internet use is pre-planned, students / 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. They include the teaching of E-Safety in their lessons
Pupils understand that there are sanctions for inappropriate use of technologies and the school will implement these sanctions in accordance with Social Media and Behaviour Policy.
Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

Designated person for Child Protection / Child Protection Officer:

The named person is trained in E-Safety issues and is aware of the potential for serious child protection issues to arise from:
Sharing personal data
Publishing of specific information relating to school based activities involving pupils, via official school systems such as the school web site, Twitter, Facebook, You Tube Sharing of school owned devices or personal devices that may be used both within and outside.
Sharing of school owned devices or personal devises that may be used in and outside of school
Access to illegal/inappropriate material
Inappropriate on-line contact with others
Potential or actual incidents of grooming
Cyber-bullying, Sexting and Radicalisation

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 / Officer (ESO)
Regular updates on the monitoring of E-Safety incident logs
Regular updates on the monitoring of the filtering of web sites
Reporting to relevant Governor committees / meetings

Students / pupils:

Students/pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure, monitored and safe system provided through DGfL. Students/pupils:
Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy/, which they will be expected to sign before being given access to school systems
Need to 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites, video streaming facilities, digital image sharing sites and cyber-bullying.
Are responsible for the safe use of school owned equipment at home, in accordance with the school AUP/AUA, for these devices. The school AUP/AUA may be used. A guardianship/loan form is available for schools to adapt for school owned equipment used by students at home.
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 the use of an externally available web based system, provided by the school
Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, may be investigated by 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 therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, parent mail website and local E-Safety campaigns.
Parents and carers will be responsible for:
Endorsing the pupil acceptable use policy
Accessing the school website / School Learning Platform/ on-line student / pupil records or other school provided system (specify here) in accordance with the relevant school Acceptable Use Policy.

Policy Statement

Education – students / pupils

There is a planned and progressive E-Safety/E-literacy curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups.
E-Safety education is provided in the following ways:

A planned E-Safety/E-literacy programme is provided as part of ICT / SMSC lessons and is regularly revisited – this include the use of ICT and new technologies in school and outside school
Key E-Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy and plausibility of information
Students / pupils are aware of the Student / Pupil AUP (AUA) and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
Rules for use of ICT systems / internet are available in the school planners and classrooms.
Students and pupils are taught the importance of information security and the need to keep information such as their password safe and secure
Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

The school provides information and awareness to parents and carers through:
Letters, newsletters, School web site.
Parents evenings, Reception/ Induction meetings.
E-Safety sessions for parents/carers
Family learning opportunities (Inspire)

The school offers E-Safety workshops so that parents and children can together gain a better understanding of these issues. Messages to the public around E- Safety are targeted towards grandparents and other relatives as well as parents.
Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training - Staff

All staff receive regular E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:
A planned programme of formal E-Safety training is made available to staff. An audit of the E-Safety training needs of all staff is carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process
All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies
The E-Safety Coordinator receives regular updates through attendance at DGfL / LA /LSGB/ other information / training and by reviewing guidance documents released by DfE / DGfL / LA, LSGB and others.
This E-Safety policy and its updates are presented to and discussed by staff in staff / team meetings / INSET days.
The E-Safety Coordinator provides advice / guidance / training as required to individuals

All staff are familiar with the schools' Policy including:
Safe use of e-mail
Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other school approved system
Safe use of school network, including the wireless network, equipment and data
Safe use of digital images and digital technologies, such as mobile phones and digital cameras
The use of mobile phones in the classroom is not allowed during the school day.
Publication of pupil information/photographs/videos/posts/blogs and information available on the school website
Capturing and storing photographs/videos/audio files on personal and school owned devices
Cyberbullying procedures
Their role in providing E-Safety education for pupils
The need to keep personal information secure
Staff are reminded / updated about E-Safety matters at least once a year.

Training – Governors

Governors take part in E-Safety training / awareness sessions,
This is offered by:
Attendance at training provided by the Local Authority / National Governors Association / DGfL/ LSGB or other relevant organisation
Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school 'managed' infrastructure / network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this document are implemented.
School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policies.
There will be regular reviews and audits of the safety and security of school ICT systems
Servers, wireless systems and cabling must be securely located and physical access restricted to authorised users.
All users will have clearly defined access rights to school ICT systems
All users will be provided with a username and password
Users will be made responsible for the security of their username and password. They 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 maintains and supports the managed filtering service provided by DGfL The school can provide enhanced user-level filtering through the use of Smoothwall filtering or a MDMs (Managed Mobile Device system)
The school manages and updates filtering issues through the RM Service desk
Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager/appropriate member of staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
Remote management tools are used by staff to control workstations and view users activity
An appropriate system is in place for users to report any actual / potential E-Safety incident to the relevant person
The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
An agreed procedure is in place for the provision of temporary access to "guests" (eg trainee teachers, visitors) onto the school system
An agreed procedure is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices
the school infrastructure and individual workstations are protected by up to date virus software
Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Curriculum

E-Safety is a focus in all areas of the curriculum. The new Computer Science Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy should be taught. Staff will re-enforce E-Safety messages in the use of ICT across the curriculum.

In lessons, where internet use is pre-planned, students / pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches.
Where students / pupils are allowed to freely search the internet, eg using search engines, staff should monitor the content of the websites the young people visit
The school provides opportunities within a range of curriculum areas to teach about E-Safety
The school teaches 'Digital Literacy' as part of the new 'Computer Science' programme of study.
It is accepted that from time to time, for good educational reasons, students 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 Network Manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying, Sexting and Radicalization and know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organization such as Childline or CEOP report abuse button.

Use of digital and video images

When using digital images, staff inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet eg on social networking sites.
Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the storing sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
Pupils permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
Students / pupils must not take, use, share, publish or distribute images of others without their permission
Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and comply with good practice guidance on the use of such images
Students' / pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs if the parent has informed the school in writing that they do not give their permission for this.

Written permission from parents or carers is obtained before photographs of students / pupils are published on the school website.

Data Protection

Personal data will is recorded, processed, transferred and made available according to the GDPR 2018

Staff are aware of the 'School Information Security Policy'. A breach of the Data Protection Act may result in the school or an individual fine of up to £500000
Staff ensure that they:
Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
Access personal data on secure password protected computers and other devices , at school and home, or via the School Learning Platform or school systems, 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

When personal data is stored on any portable computer system, USB stick or any other removable media:
The data must be password protected
The devise must have relevant virus software
The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

When using communication technologies the school considers the following as good practice:
The official school email service may be regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems eg by remote access from home.
Users need to be aware that email communications may be monitored
Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email

Any digital communication between staff and students / pupils or parents / carers (email, chat, dojo points etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. **Personal** email addresses, text messaging or public chat / social networking programmes must not be used for these communications

Students / pupils are provided with individual school email addresses for educational use.

Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.

Staff are not allowed to use their mobile phones in the classroom during teaching hours and lunch breaks. Staff are allowed to use them during breaks in designated staff areas only such as the staff room and the offices.

The school is not responsible for the loss, damage or theft of any personal mobile device thus pupils are discouraged to bring them into school. If they do they are taken to the school office and a parent/carer needs to collect them.

The sending of inappropriate text messages between any member of the school community is not allowed

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with GDPR 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-Safety is a key focus. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

Informing parents or carers.

Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).

Referral to LA or Police.

The LA has set out the reporting procedure for E-Safety incidents (see Appendix 1).
Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.
Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
Complaints related to child protection are dealt with in accordance with school child protection procedures.