Fosse Primary School

ESafety Policy

INTRODUCTION

Fosse Primary School recognises that the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning. 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 eSafety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- inclusion in the National Education Network which connects all UK schools (The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content);
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

To enable this to happen, we have taken a whole school approach to ESafety as promoted by the British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

Fosse Primary School, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow SEND pupils increased access to the curriculum and other aspects related to learning.

Fosse Primary School is committed to ensuring that all its pupils will be able to use existing, as well as upcoming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.

In addition, staff teach internet safety to pupils through the Purple Mash computing scheme of work, PSHE and termly internet safety assemblies.

The nominated senior person for the implementation of the School's eSafety policy is the Headteacher, Richard Stone.

SCOPE OF POLICY

The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

Fosse Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for ESafety;
- available information to parents that highlights safe practice for children and young people when using the Internet, Virtual Learning Environments (VLE) and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the Internet, VLE and digital technologies;
- education that is aimed at ensuring safe use of Internet, VLE and digital technologies;
- a reporting procedure for abuse and misuse.

INFRASTRUCTURE AND TECHNOLOGY

Partnership working

Fosse Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. Some of our major partners include eSafety4Schools and Virgin Media for Business who provide the network, services and facilities that support the communication requirements of our school.
As part of our commitment to partnership working, we fully support and will continue to work with eSafety4Schools to ensure that pupil and staff usage of the internet and digital technologies is safe.

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the eSafety coordinator or IT Technician who will then contact the eSafety4Schools helpdesk.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system such as those used by PurpleMash.
- Pupils must immediately tell a teacher or click the report email button in PurpleMash if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully in the same way as a letter written.
- The forwarding of chain letters is not permitted.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

All internet content is filtered using eSafety4Schools web filtering service at a level appropriate for Primary School usage; this is also monitored by IT Solutions 4 All using a monitoring software called Securus. The Headteacher is notified directly when there are any concerns which are also shared with Maclean Data who provide IT support for the school.

Portable Technologies:

- The use of portable devices such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Memory sticks used in school will need to be encrypted, the office can provide you with one if required.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile phones in school.
- Staff should not use personal mobile phones during designated teaching sessions – permission will be granted by the Headteacher, in exceptional circumstances, for staff to leave their mobile switched on.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.

Use of iPads

iPads are used for digital storytelling, internet research, and to support learning and teaching across the curriculum via the use of a range of appropriate apps. Only staff are to collect and return jPads and only staff in school will know the code to unlock the cabinet for the iPads. Children will be monitored as closely as possible using the mobile devices with the previously mentioned filtering system also in place.
When using iPads, children will be reminded to be Internet Wise and apply the SMART Internet safety rules. They will not be allowed to use iPads to:

- Take photos of pupils/staff without permission or direction from the teacher.

POLICIES AND PROCEDURES

We at Fosse Primary School understand that effective policies and procedures are the backbone to developing a whole-school approach to eSafety. The policies that exist within Fosse Primary School are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils.

Introducing the eSafety Policy to pupils

- eSafety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during computing lessons, circle times, anti-bullying week, Internet Safety Workshops and assemblies
- Pupils will be informed that network and Internet use will be monitored**.**

Staff and the eSafety Policy:

- All staff will be informed about and given access to the School eSafety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will be involved in discussions regarding eSafety and will have a copy of the eSafety Policy.
- Staff will be aware that Internet use can be monitored and traced to the individual. Professional conduct is essential.

- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone where contact with pupils or parents is required

Staff should follow the guidelines below:

- Never communicate with pupils outside of school.
- Never respond to informal, social texts from pupils.
- Never use personal devices to take images or videos of children.

Communication of Policy to Parents

- Parents' attention will be drawn to the School eSafety Policy in newsletters, the school prospectus and on the school Web site.

Use of Internet facilities, mobile and digital technologies

Fosse Primary School will seek to ensure that Internet, VLE, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

Fosse Primary School expects all staff and pupils to use the Internet, VLE, mobile and digital technologies responsibly and strictly according to the conditions below: These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material

The School recognises that in certain planned curricular activities, access to potentially 'blocked' sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and also permission is given by senior leaders, so that the action can be justified, if queries are raised later.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy

- Other criminal activity

In addition, users may not:

- Use internet service provider's facilities for running a private business.
- Enter into any personal transaction that involves the Local Authority or service provider in any way.
- Visit sites that might be defamatory or incur liability on the part of Local Authorities, service providers or Fosse Primary School itself.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Fosse Primary School
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services.
- Undertake activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the school network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - continuing to use an item of networking software or hardware after IT support has requested that use cease.
    - other misuse of the school network, such as introduction of viruses.
- Use any mobile or digital technologies or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Where Virgin Media (provider of Internet connectivity and associated services to schools) and/or eSafety4Schools become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

Reporting Abuse

There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately to the Headteacher, Richard Stone.

The School also recognises that there will be occasions where pupils may be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances Local Authority Safeguarding Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures assist and provide information and advice in support of child protection enquiries and criminal investigations.

Cyber Bullying

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites. If it takes place within school, cyberbullying will be dealt with in line with the school's overall anti-bullying policy, discipline policy and pastoral services.
In our school children will be taught:

- If they feel they are being bullied by e-mail, through social networking sites, text or online they should always tell someone they trust.
- Not to reply to bullying, threatening text messages or e-mails as this could make things worse.
- Not to send or forward abusive texts or e-mails or images to anyone.
- Keep abusive messages as evidence.

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school

We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

EDUCATION AND TRAINING

Fosse Primary School recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

As part of achieving this, we want to create within Fosse an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

To this end Fosse Primary School will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

STANDARDS AND INSPECTION

Fosse Primary School recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

Monitoring

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet, VLE and electronic mail a pupil or member of staff may have. Fosse Primary School recognises that in order to develop an effective whole school eSafety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

With regard to monitoring trends, within the school and individual use by school staff and pupils, Fosse Primary School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

Use of the school's computers and access to the internet is monitored using Securus Software's Securus XT program, administered on behalf of the school by IT Solutions 4 All. Securus looks at the usage of all devices that access the school network and reports back to the school should any violation of our eSafety policy occur.

All internet content is filtered using 'iBoss web filtering' at a level appropriate for Primary School usage; this is also monitored by IT Solutions 4 All. The head teacher is notified directly when there are any concerns which are also shared with Maclean Data who provide IT support for the school.

Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently subjected to harm.

Handling eSafety Complaints:

- Complaints of Internet misuse will be dealt with by principal/senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the eSafety incident logbook.
- As part of the Acceptable Use Agreement children will know that if they deliberately break the rules they could be stopped from using the internet or computer and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Complaints regarding cyberbullying will be dealt with in line with the school Anti-Bullying Policy.
- Pupils and parents will be informed of the complaints' procedure.
- Any complaint about staff misuse must be referred to the head teacher and governors.

WORKING IN PARTNERSHIP WITH PARENTS AND CARERS

Fosse Primary School is committed to working in partnership with parents and carers and understand the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

At Fosse Primary School we also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

We remind parents through newsletters and text about eSafety issues and any new developments as they arise. For example, we remind parents that pupils under the age of thirteen should not have access to Facebook accounts.

Appendix 1 2020 Blended Learning Policy Fosse Primary School

1. Online safety

1.1. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.
- Staff will host recorded and/or live lessons where and when they find this will enhance the learning experience for the pupils of Fosse Primary School.
- If recorded and/or live lessons are used these will be for up to 2.5 hours daily.
- Staff will send the invite to the pupils for the live lesson the morning of the scheduled lesson.
- Ensure no other family members are on view of the camera.
- Ensure they conduct all videoing with a plain background.
- No live videos to be conducted outside the hours of 8.50am to 3.00pm.

1.2. All staff and pupils using audio visual communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

1.3. The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

1.4. Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

1.5. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

1.6. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

1.7. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can

recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

1.8. The school will communicate to parents via email and phone calls about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

1.9. During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

1.10. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

1.11. Please also see the 'Acceptable Use Policy for Live Lessons during the Coronavirus pandemic' for further information regarding Live and recorded lessons.

Policy	**ESafety Policy**
Reviewing Committee	**Policy Committee (Review and Standards Committee)**
Reviewed	**October 2020**
Ratified by Governing Body	
Signed	
Date of next review	**September 2021**