Staff responsible	Andy Taylor
Date of policy/last review	31/05/2017
Governing body ratified	22/05/2018
Chair of Governors	
Review cycle	2 years
Next review	31/05/2019

1. Purpose

1.1 The Headteacher and Governing Body have a legal responsibility to safeguard children and staff and this includes online activity.

2. Teaching and learning

2.1 Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

2.2 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 functions. Internet access is an entitlement for all pupils.

2.3 Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

2.4 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.5 How will pupils learn how to evaluate Internet content?

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will use age-appropriate tools to research Internet content.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

3. Managing Information Systems

3.1 How will information systems security be maintained?

The Server must be located securely and physical access restricted.

- The server operating system must be secured and kept up to date.
- Virus protection for the whole network has been installed and will be kept current.
- Access by wireless devices will be proactively managed and secured with a minimum of WPA2 encryption.

The Schools Broadband network is protected by a cluster of high performance firewalls provided by LGFL.

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

3.2 How will email be managed?

LGFL currently filter some spam and unrecognised email.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

3.3 How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

The Head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.4 Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.
- Parents/Carers will be specifically asked to give their written permission for images to be published online or in the local media at the admissions interview.

3.5 How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- If staff or pupils discover unsuitable sites, the URL will be reported and then record the incident and escalate the concern as appropriate.
- Any material that the school believes is illegal will be reported to SLT.

3.6 How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- The equipment must be secure and if necessary locked away when not in use.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

3.7 How are emerging/new technologies managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Pupils will be instructed about safe and appropriate use of personal devices

3.8 How will Internet access be authorised?

- All staff will read and sign the 'Acceptable Use Agreement' Policy before using any school ICT resources.
- All visitors to the school site who require access to the school's network or internet access will be reminded of the Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

4. How should personal data be protected?

4.1 The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

4.2 Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

4.3 The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

4.4 Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

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

5. Curriculum access

5.1 It is difficult to articulate the level of adult supervision that pupils require whilst using the Internet as this is dependent upon their individual abilities which are not age bound.

5.2 As in all areas of school life it is hoped that as pupils progress through the school they can access with increasing independence aware of their responsibilities and adhering to safe practise.

5.3 Internet usage within school for all users is monitored and where sites are being used for purposes other than Teaching and Learning filters may be applied to prevent access.

6. How will risks be assessed?

6.1 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

6.2 The SLT will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

6.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches may be reported to the Police.

6.4 Methods to identify, assess and minimise risks will be reviewed regularly.

7. How will the school respond to any incidents of concern?

7.1 All members of the school community will report e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc.) to the SLT.
7.2 The school will record all reported incidents and actions and other in any relevant areas e.g. Bullying or Child protection log.
7.3 The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
7.4 The school will inform parents/carers of any incidents of concerns as and when required.
7.5 After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
7.6 Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
7.7 If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the LA IT lead.

8. How will e–Safety complaints be handled?

8.1 Complaints about Internet misuse will be dealt with under the school's complaints procedure.
8.2 Any complaint about staff misuse will be referred to the Head teacher.
8.3 All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
8.4 Pupils and parents will be informed of the complaints procedure.
8.5 Parents and pupils will need to work in partnership with the school to resolve issues.
8.6 All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
8.7 Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures. All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

9. How will Cyber bullying be managed?

9.1 Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

9.2 Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects.
It is essential that young people, school staff and parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

9.3 There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents

- Gives head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

9.4 Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

9.5 Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

9.6 Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
There are clear procedures in place to support anyone in the school community affected by cyber bullying-contact the Head teacher
All incidents of cyber bullying reported to the school will be recorded.
Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos.

9.7 Sanctions for those involved in cyber bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

10. Providing Information

10.1 Informing pupils of the contents of this policy:
All users will be informed that network and Internet use will be monitored.

- Pupil instruction regarding responsible and safe use will precede Internet access.
- E-Safety rules will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

10.2 Informing staff of the contents of this policy:
The e–Safety Policy will be formally provided to and discussed with all members of staff.

- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could

be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

10.3 Informing Parents of the contents of this policy:

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks.

Parents' attention will be regularly drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.

- A partnership approach to e-Safety at home and at school with parents will be encouraged.
- Parents will be encouraged to read the school rules for using the internet and discuss its implications with their children.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents on request.