CONTENTS Page

1.0 INTRODUCTION

Our e-Safety Policy has been written by the Head Teacher, taking into account government guidance.

It has been agreed by the senior management team. The e-Safety Policy and its implementation will be reviewed annually.

Implementation: It is the responsibility of line managers to ensure that staff members are aware of and understand this policy and any subsequent revisions.

Compliance: This policy complies with all relevant regulations and other legislation as detailed in the *Compliance with Regulations & Legislation Statement*.

2.0 THE IMPORTANCE OF INTERNET USE

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.

Internet use is part of the statutory curriculum and a necessary tool for learning.

Internet access is available for all students providing they show a responsible and mature approach to its use. **It can be withdrawn if and when misused.**

The Internet is an essential element in 21st Century 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.

Students use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of the Internet to education:

- Access to world-wide educational resources including museums and art galleries;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students 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 DfE;

- Access to learning wherever and whenever convenient;

Using the Internet to enhance learning:

The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students;

Students 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. Access levels will be reviewed to reflect the curriculum requirements and age of students;

Staff should guide and supervise students in on-line activities that will support the learning outcomes planned for the students' age and maturity;

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;

Evaluation of Internet content:

The school will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law;

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;

Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work;

The evaluation of on-line materials is a part of most subjects;

3.0 MANAGING INFORMATION SYSTEMS

Information system security:

- Security strategies will be discussed with the school's ICT support team regularly;
- The school's server will be backed up to an offsite location each night. This is managed by centralised ICT support at Head Office;
- Anti-Virus protection will be updated regularly;
- The security of individual staff and student accounts will be reviewed regularly;
- The administrator account password will be changed if it becomes known;
- Computers (including mobile devices or additional hardware) may not be connected to the school network both physically or wirelessly without specific permission;
- Personal data sent over the Internet will be encrypted or otherwise secured;
- Portable media may not be used without specific permission followed by a virus check;
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail;
- Files will not be moved or removed from a shared folder without specific permission;

- Personal data will not be stored on school servers without specific permission. Files held on the school's network will be regularly checked;
- Software will not be installed/removed from computers without specific permission;
- The network manager will review system capacity regularly

E-mail:

- Students may only use approved e-mail accounts and these are set up and managed by the ICT coordinator for use as part of their course of study;
- Students must immediately tell a teacher if they receive offensive e-mail;
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;
- Whole-class or group e-mail addresses should be used in the primary area;
- Access in school to external personal e-mail accounts may be blocked;
- Excessive social e-mail use can interfere with learning and will be restricted;

Management of published content:

- The contact details on the website should be the school address, e-mail and telephone number. Staff or students' personal information must not be published;
- E-mail addresses should be published carefully, to avoid spam harvesting;
- The Head Teacher, in conjunction with Outcomes First Group will take overall editorial responsibility and ensure that content is accurate and appropriate;
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright;

Publishing of student images:

- Students also need to be taught the reasons for caution in publishing personal information and images in social publishing sites (see section 3.5).
- Images that include students will be selected carefully and will have parental consent to be published;
- Written permission from parents or carers will be obtained before images of students are electronically published by the school. All parents and carers are sent consent forms regularly and a database of permissions updated;
- Written permission from the school should be obtained before students or parents/ carers publish images taken from the school website or of school events;
- Work can only be published with the permission of the parents/ carers and, when appropriate, pupils;

Management of social networking and personal publishing:

Examples include: blogs, wikis, Facebook, Twitter, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The school will block/ filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone

numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.

- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school;
- Teachers should be advised not to run social network spaces for student use on a personal basis.
- Teachers are advised that the Company does not authorise personal blogs to be linked to the school. Please see Outcomes First Group Internet Usage policy;
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others;
- Students should be advised not to publish specific and detailed private thoughts;
- Students should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments;

Web Filtering:

- The school will work with Head Office and external organisations as relevant to ensure that systems to protect students are reviewed and improved;
- If staff or students discover unsuitable sites, the URL must be reported to the e-Safety Coordinator;
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Any material that the school believes is illegal must be reported to appropriate agencies such as Police and the IT personnel;
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the students, advised by engineers;

Emerging Technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden;
- The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on phone use in school;
- Staff will be issued with a school phone where contact with students is required;

Protection of personal data:

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

4.0 POLICY DECISIONS & RISK ASSESSMENT

Authorisation to use the Internet:

The school will maintain a current record of all staff and students who are granted access to the school's electronic communications;

All staff must read and sign the Outcomes First Group policy for internet usage before using any school ICT resource;

At Key Stage 1/2, access to the Internet will be by adult demonstration with some directly supervised access to specific, approved on-line materials;

Secondary students must apply for Internet access individually by agreeing to comply with the e-Safety Rules;

Parents will be informed that students will be provided with supervised Internet access.

Risk Assessment:

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 nor Outcomes First Group can accept liability for the material accessed, or any consequences resulting from Internet use;

The school audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate;

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990;

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

5.0 GENERAL

Communications Policy:

- E-Safety rules will be posted in rooms with Internet access;
- Students will be informed that network and Internet use will be monitored;
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede Internet access;
- An e-safety module will be included in the PSHCE and ICT programmes covering both school and home use;

Staff sharing of e-safety policy:

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required;

Parental involvement

- Parents/carers' attention will be drawn to the school's e-Safety Policy in newsletters, the school prospectus and on the school website;
- Internet issues will be handled sensitively, and parents/ carers will be advised accordingly;
- E-safety awareness workshops will be provided as part of Parents evening on both the primary and secondary sites;

- A partnership approach with parents/ carers is well established and encouraged;
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents/ carers.

E-Safety Contacts and References:

BBC Chat Guide

http://www.bbc.co.uk/chatguide/

Becta

http://www.becta.org.uk/schools/esafety

Childline

http://www.childline.org.uk/ ***Childnet*** http://www.childnet-int.org ***Kidsmart*** http://www.kidsmart.org.uk ***Digizen***

http://www.digizen.org/cyberbullying/film.aspx

Child Exploitation & Online Protection Centre

http://www.ceop.gov.uk

e-Safety in Schools

http://www.clusterweb.org.uk?esafety

Grid Club and the Cyber Cafe

http://www.gridclub.com

Internet Watch Foundation

http://www.iwf.org.uk/

Internet Safety Zone

http://www.internetsafetyzone.com/

West Sussex e-Safety Pages http://wsgfl.westsussex.gov.uk/ccm/navigation/learners/stay-safe/bullying/e-safety-in-west- sussex-schools/

Kidsmart

http://www.kidsmart.org.uk/

NCH – The Children's Charity

http://www.nch.org.uk/information/index.php?i=209

NSPCC

http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Stop Text Bully

www.stoptextbully.com

Think U Know website

http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse

http://www.virtualglobaltaskforce.com/

Document Type	Policy	**Version Number**	1.0
Policy Owner	Headteacher	**Last Review Date**	June 2017
Date First Issued	June 2017	**Next Review Date**	At least annually

Document Type	Policy	**Version Number**	1.0
Policy Owner	Headteacher	**Last Review Date**	June 2017
Date First Issued	June 2017	**Next Review Date**	At least annually