ROWDEFORD SCHOOL

POLICY ON INTERNET USE AND E-SAFETY

This policy should be read in conjunction with the following policies: Computing Curriculum; Personal Use of Social Media; Secure Data Handling; Lettings; Use of Email by Staff

RATIONALE FOR INTERNET USE IN SCHOOL

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.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, wellbeing and to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

ROLES AND RESPONSIBILITES:

THE ROLE OF THE COMPUTING COORDINATOR (Sarah Curwen)

- To help and support colleagues in the use and teaching of the internet through the Computing curriculum;
- To ensure Responsible Internet Use and E-safety are covered in the relevant Computing Schemes of Work;
- To keep up-to-date with developments in internet and mobile technology;
- To organise and lead relevant in-service training and meetings.

THE ROLE OF THE BUSINESS MANAGER (Rachel Lambert)

- To ensure that non-educational users of the school's internet are made aware of the policy on internet access;
- To coordinate a response to illegal and/or suspicious content that is discovered on the school's network;
- To sample network usage and logs;
- To approve access where requested to sites previously filtered;

THE ROLE OF THE INTERNET SERVICE PROVIDER (Oakford Internet Services)

- To provide a filtered Internet connection with a flexibility for Rowdeford School to make changes to the filtering rules as deemed necessary.

1 HOW WILL INTERNET USE ENHANCE LEARNING?

1.1 The school internet usage is designed for educational use and includes filtering appropriate to the age of pupils.

1.2 Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

1.3 Pupils are taught appropriate internet use and are given clear objectives for internet use. They are taught how to use the internet for research, including the skills of knowledge location, retrieval and evaluation.

2 HOW INTERNET ACCESS IS AUTHORISED

2.1 Students are required to sign Responsible Internet Use Agreements at the start of each school year when they receive their annual School Planner ;

2.2 Parents are informed that pupils only have supervised internet access and are also asked to sign the Responsible Internet Use Agreement at the start of each school year;

2.3 Community users of the school's IT facilities (e.g. for lettings, training and other non-educational activity) must confirm acceptance of the school's Acceptable Use Policy. In the case of lettings, appropriate wording will be included in the Letting's Booking Form. A copy of this policy will be made available to all other users.

3 MANAGING INTERNET FILTERING

3.1 The school works in partnership with parents, and Oakford Internet Services (OIS) to ensure systems to protect pupils are regularly reviewed and improved;

3.2 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported by email to the Internet Service Provider (OIS) at support@oakfordis.com (the Business Manager should be copied into any such notifications to track the response)

3.3 Website logs are sampled and monitored by the School Business Manager;

3.4 The Computing Coordinator will send regular reminders concerning Internet Safety to staff;

3.5 Any material that the school believes is illegal must be referred by a member of the Senior Leadership Team to Internet Watch Foundation;

3.6 Members of staff will be automatically provided with a separate set of filtering rules allowing less restrictive access to the Internet. The connection will still be filtered based on the underlying rules as set by the Internet Watch Foundation.

4 MANAGING CONTENT

4.1 HOW WILL PUPILS LEARN TO EVALUATE INTERNET CONTENT?

4.1.1 Specific lessons are included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources. Where appropriate, pupils are taught to acknowledge the source of information used and to respect copyright when using internet material in their own work;

4.1.2 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported via email to OIS at support@oakfordis.com

4.1.3 Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law. Training is available to staff in the evaluation of web materials and methods of developing students' critical attitudes;

4.1.4 The Computing Coordinator will be responsible for recommending the permission of additional websites as requested by colleagues to leadership/ the Business Manager for final instruction.

4.2 HOW SHOULD THE SCHOOL'S WEBSITE CONTENT BE MANAGED?

4.2.1 The point of contact on the website is the school address, school e-mail and telephone number. Staff or pupils' home information are never published;

4.2.2 Written permission from parents or carers will be obtained before photographs of pupils are published on the externally accessible sections of the school's website.

4.2.3 Website photographs that include pupils are selected carefully in line with the relevant permission being given and do not enable individual pupils to be clearly identified;

4.2.4 Pupils' full names should not be used anywhere on the website;

4.2.5 Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified.

5 COMMUNICATION

5.1 MANAGING PUPILS' EMAIL

5.1.1 Pupils may only use e-mail accounts at school which have been approved by the teacher taking the lesson;

5.1.2 Pupils must immediately tell a teacher if they receive offensive or suspicious e-mail. This information must then be passed to the Curriculum Coordinator who will notify the Oakford support desk who are able to modify the settings to allow for some tracking of the message. This should always be supervised by a senior member of school staff.

5.1.3 Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone;

5.1.4 Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly;

5.1.5 Access in school to external personal e-mail accounts may be blocked;

5.1.6 Excessive social e-mail use can interfere with learning and may be restricted;

5.1.7 E-mail sent to an external organisation should be written carefully, and must not be in breach of the Data Protection Act (1999);

5.1.8 Information is available to parents explaining how students can access their accounts from home.

5.2 ONLINE COMMUNICATIONS AND SOCIAL NETWORKING

5.2.1 Pupils are taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety;

5.2.2 The school conducts regular pupil and parent surveys about home use of ICT. The results gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.;

5.2.3 The use of online chat is not permitted in school, other than as part of its online learning environment;

5.2.4 Staff are permitted to use Social Media sites at certain times during the working day: see the Personal Use of Social Media policy

6 MOBILE TECHNOLOGIES

6.1 Pupils' personal mobile phones are not permitted during the school day (subject to point 6.2). These are collected in at the start of the school day and returned during taxi time.

6.2 Appropriate use of mobile phones will be taught to pupils as part of their PSHE programme and within the KS4 Computing Scheme of Work.

6.3 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Curriculum Coordinator and/or School Business Manager before use in school is allowed.

6.4 The sending of abusive or inappropriate text messages is forbidden.

7 INTRODUCING THE E-SAFETY POLICY TO PUPILS

7.1.1 Each year, a module on Responsible Internet Use and E-safety is included in the Computing curriculum covering both school and home use. This includes the necessity of keeping personal information safe, how to use mobile technologies and using online communication appropriately;

7.2 Rules for internet access are posted in all rooms where computers are used;

7.3 Pupils are informed that internet use is monitored;

7.4 The school uses relevant, up-to-date resources to teach and reinforce understanding about Responsible Internet Use and E-safety.

8 PARENTS AND E-SAFETY

8.1 Parents' attention is regularly drawn to the School's E-Safety Policy in newsletters, the school brochure and on the school Website;

8.2 Information will be available to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children.

9 STAFF AND THE E-SAFETY POLICY

9.1 All staff including teachers, supply staff, classroom assistants and support staff, are provided with the School Internet and E-Safety Policy and its importance explained;

9.2 The school's consequences for internet and mobile phone/PDA/technology misuse are clear so that all teachers are confident to apply this should the situation arise;

9.3 All staff will follow the terms of the 'Responsible Internet Use' statement before using any internet resource in school;

9.4 Staff are made aware that internet traffic is monitored and reported by OIS and can be traced to the individual user. Discretion and professional conduct is essential;

9.5 Staff development in Safe and Responsible Internet Use and on the school internet policy will be provided as required.

10 COMPLAINTS PROCEDURE

10.1 Responsibility for handling pupil IT-related incidents is delegated to the Senior Leadership Team;

10.2 Any complaint about staff IT misuse must be referred to the Headteacher;

10.3 The school's Complaints Procedure is published on the website and in the school prospectus;

10.4 Parents and pupils need to work in partnership with staff to resolve issues;

10.5 There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. In such cases, a Senior member of staff must be informed;

10.6 Sanctions available for pupils include:
- interview/counselling by tutor or key worker
- 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

10.7 Sanctions available for staff include:

Disciplinary action

In the most severe cases, could lead to dismissal

11 POLICY REVIEW

This Policy will be reviewed on an annual basis by the Business Manager and by the Governing Body, in line with the school's Policy Review Schedule.

This policy was reviewed in January 2017 and endorsed by the Governing Body at their meeting of 27 March 2017

Signed …… Date ……
Clerk to the Governors