Acceptable Use

Internet Safety Policy

Christ Church & Holy Trinity CE Primary Schools Federation

2019-21

Why is Internet access important?

The purpose of the Internet in school is to increase the opportunities for pupils to access a wider range of resources in support of the curriculum

It supports the professional work of staff and enhances the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and pupils. It is an entitlement for all pupils as it helps them to develop a responsible and mature approach to accessing information.

What are the benefits to the School?

The Government has set targets for ICT use in all schools by 2005 through the ICT in Schools (formerly National Grid for Learning) Initiative. A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as NGfL, the Virtual Teacher Centre, Regional Broadband Consortia;
- Information and cultural exchanges between students world-wide;
- News and current events;
- Cultural, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for pupils and staff;
- Staff professional development - access to educational materials and good curriculum practice; Communication with the advisory and support services, professional associations and colleagues;
- Exchange of curriculum and administration data with the LEA and DfES

How will the school ensure Internet use provides effective learning?

- Curriculum planning will identify opportunities to enrich and extend learning activities via access to the Internet;
- Pupils will be given clear objectives for Internet use;
- Pupils will be provided with lists of relevant and suitable Web sites;

- Pupils will be informed of their responsibilities;
- Pupils will be informed that checks can be made on files held on the system;
- Pupils using the Internet will be supervised appropriately;
- Internet access will be purchased from a supplier that provides a service designed for pupils. This will include filtering appropriate to the age of pupils;
- The school will work with the LEA and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.

How will pupils be taught to assess Internet content?

Appropriate to their age and experience:

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Pupils will be taught to validate information before accepting it as true, and to discriminate between fact and opinion;
- When copying materials from the web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed;
- Pupils will be taught Internet content issues, for instance the value and credibility of web materials in relationship to other media;
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable;
- Children will be encouraged to use the Internet to enhance rather than replace existing methods of research.

How will Internet access be authorised?

Internet access is a necessary part of statutory curriculum. It is an entitlement for students based on responsible use.

- Parents will be informed that students will be provided with monitored Internet access;
- Parents will provide permission for their child to access the Internet;

- Pupils [Key Stage 2 upwards] will agree individually to the Rules of Responsible Use / Acceptable Use.
- This policy will be made available to parents;
- A record will be maintained of all students with Internet access.
- Staff and students will be removed from the record when access is no longer required, or is withdrawn.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The School will supervise students and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks will be reviewed;
- Staff, parents, governors and advisers will work to establish an agreement that every reasonable measure is being taken.

- The Head Teacher will ensure that the policy is implemented effectively.

How will the School ensure Internet access is safe?

- The school will work in partnership with the LEA, DfES, parents, and the Regional Broadband / Internet Service Provider to ensure systems to protect students are reviewed and improved;
- All users will be informed that Internet use will be monitored;
- Systems Administrators will ensure that regular checks are made to ensure that the filtering methods selected are effective in practice;
- Pupils will not have access to Internet logs;
- Any failure of the filtering systems will be reported directly to the Systems Administrators;

- The school reserves the right to remove access to any website it considers inappropriate;
- If staff or students discover unsuitable sites, the URL (address) and content will be reported to the network manager / ICT coordinator, London Grid for Learning (LGfL) or LEA as appropriate;
- Any material that the school suspects is illegal will be referred to the appropriate authorities.

The Internet is a communications medium that is freely available to any person wishing to publish a Website with no editorial intervention. While access to appropriate information should be encouraged, pupils will generally need protected access to the Internet. The level of protection will be appropriate to the needs of the pupil.

How will the security of the school ICT system be maintained?

- The ICT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use;
- The whole system will be reviewed with regard to threats to potential threats from Internet access;
- No personal data should be sent over the Internet unless it is encrypted or otherwise secured;
- Virus protection will be installed and updated regularly;
- Personal floppy disks may not be brought into school without specific permission and must be virus checked.

How will e-mail be managed?

From Key Stage 2, pupils are expected to use E-mail as part of the National Curriculum.
- The school will provide group or individual email addresses as meets educational needs;
- Communications with persons and organizations will be managed to ensure appropriate educational use and that the good name of the school is maintained;

- The forwarding of chain letters will be banned;
- Pupils may send e-mail as part of planned lessons only;
- E-mail messages on school business (e.g. arranging a work placement) must be approved before sending.
- Pupils will only be given 'safe' email accounts through the London Grid for Learning or other approved Supplier, being Christ Church's own Microsoft office 365 account. (Domain name: chchchristchurch.rbkc.sch.uk).

How will publishing on the Web be managed?

- The Head teacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained;
- The Web site will comply with the school's guidelines for publications;
- Pupils will be taught to publish for a wide range of audiences which might include governors, parents or young children;
- All material must be the author's own work, credit the sources used and state clearly the author's identity or status;
- The point of contact on the Web site will be the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the Web will not have names attached.
- Parental / guardian permission will be gained for use of a child's photograph.

How will incidents be handled?

The management of the Acceptable Use of the Internet in school is achieved by:

- Protection software installed on the network;
- Acceptable Use Policy adopted by the school;
- Staff contracts signed by all staff;
- A range of disciplinary procedures for infringements of the policy.

Whenever a student or staff member infringes the policy, the final decision on the level of sanction will be at the discretion of the school management.

Pupils

Category A infringements

- Use of non-educational sites during lessons
- Unauthorized use of email

[Possible Sanctions – referred to class teacher]

Category B infringements

- Continual use of non-educational sites during lessons after being warned
- Unauthorized use of email after being warned
- Use of chat rooms or newsgroups

[Possible Sanctions – referred to Head of Department / tutor / removal of Internet access rights for a period]

Category C infringements

- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
- Transmission of commercial or advertising material
- Deliberately corrupting or destroying others' data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature
- Any purchasing or ordering of items over the internet

[Possible Sanctions – referred to Head of Department / tutor / Head teacher / removal of Internet access rights for a period / possibly letter to parents]

Category D infringements

- Continued sending of emails regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion]

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping.

[Sanction - referred to line manager.]

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules (such as misusing passwords);
- Breaching a software copyright or license;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Sanction – Referred to Head teacher / Governors with disciplinary procedures]

If a member of staff commits an exceptionally serious act of gross misconduct they may be instantly dismissed without notice. Normally, though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that, they will be asked to explain their actions and these will be considered before any disciplinary action is taken.

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called: see the free phone number at: http://content.met.police.uk/Site/childprotection

How will staff and students be informed?

- All staff will sign our school O365 Email and Internet Usage Form;
- All staff will be provided with the Internet Access Policy and its importance explained;
- All teachers will sign an AUP;
- Pupils will be taught about responsible Internet use and given rules for using the Internet, email and computer network; [Older pupils will sign an AUP];
- The school's policy will be made available to parents.

Signed: *Avis Hawkins*   *November 2019*

	Name of School	Christ Church & Holy Trinity CE Primary Schools
	Policy review Date	November 2019
	Date of next Review	November 2021
	Who reviewed this policy? Ratified by the Full Governing Body	Full Governing Body, Achievement Committee and Avis Hawkins November 2019