

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

1 Why is ICT important?

- 1.1 ICT (Information and Communication Technology) at the Ryes College increases the opportunities for learners to access a wide range of resources in support of the curriculum and learning. It supports the professional work of staff and enhances the school's management of information and business administration practice.
- 1.2 Access to the network and the Internet is necessary for staff and learners. It is an entitlement for all learners as it helps them to develop a responsible and mature approach to accessing information.

2 What are the benefits to the School?

- 2.1 The Learning Platforms Framework Agreement delivered access to a virtual learning space for all schools following a number of studies and government projects that indicated the benefits to be gained through the appropriate use of the ICT systems including the Internet in education.
- 2.2 These benefits include:
 - 2.2.1 Access to world-wide educational resources including museums and art galleries;
 - 2.2.2 Information and cultural exchanges between learners world-wide;
 - 2.2.3 News and current events;
 - 2.2.4 Cultural, social and leisure use in libraries, clubs and at home;
 - 2.2.5 Discussion with experts in many fields for learners and staff;
 - 2.2.6 Staff professional development - access to educational materials and good curriculum practice;
 - 2.2.7 Communication with the advisory and support services, professional associations and colleagues;
 - 2.2.8 Exchange of curriculum and administration data with the LA and DfE, using correct security procedures.

3 How will the School ensure Internet use provides effective learning?

- 3.1 Curriculum planning will identify opportunities to enrich and extend learning activities via access to the Internet;
 - 3.1.1 Learners will be given clear objectives for Internet use;
 - 3.1.2 Learners will be provided with access to relevant and suitable Web resources;
 - 3.1.3 Learners will be informed that checks can be made on files held on the system;
 - 3.1.4 Learners using the Internet will be supervised appropriately;
 - 3.1.5 Internet access will be purchased from a supplier that provides a service designed for learners.

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

3.2 This will include filtering appropriate to the age of learners;

3.2.1 The school will work with statutory Authorities and the Internet Service Provider to ensure systems to protect learners are regularly reviewed and improved.

4 How will learners be taught to assess Internet content?

4.1 ICT teaching incorporates Internet content issues, for instance the value and credibility of Web materials in relationship to other media

4.2 Learners will be taught to validate information before accepting it as true, and to discriminate between fact and opinion

4.2 When copying materials from the Web, learners will observe copyright and plagiarism rules

4.3 Learners will be made aware that the writer of an e-mail or the author of a Web page may not be the person claimed

4.4 Learners 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;

4.5 Learners will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

4.6 Young Learners will be encouraged to use the Internet to enhance rather than replace existing methods of research

5 How will Internet access be authorised?

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

5.2 Parents will be informed that young learners will be provided with monitored Internet access.

5.3 Learners must apply for Internet access individually, which is then authorised and monitored.

6 How will the risks be assessed?

6.1 In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for learners. The School will supervise learners and take all reasonable precautions to ensure that users access only appropriate material. However, due to the

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

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.

6.2 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

6.3 Methods to identify, assess and minimise risks will be reviewed

6.4 Staff, parents and carers will work to establish agreement that every reasonable measure is being taken

7 How will the School ensure Internet access is safe?

7.1 All users will be informed that Internet use will be monitored

7.2 Any failure of the filtering systems will be reported directly to the Network Manager

7.3 The School reserves the right to remove access to any website it considers inappropriate

7.4 The School will work in partnership with parents, the statutory authorities, DFE and the Internet Service Provider to ensure systems to protect learners are reviewed and improved

7.5 The Headteacher will ensure that regular checks are made to ensure that the filtering methods selected are effective in practice

7.6 If staff or learners discover unsuitable sites, the URL (address) and content will be reported to the network manager

7.7 Any material that the School suspects is illegal will be referred to the appropriate authorities

7.8 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, learners will generally need protected access to the Internet. The level of protection will be appropriate to the needs of the learner.

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

8 How will the security of the School ICT system be maintained?

- 8.1 The whole system will be reviewed with regard to threats to potential threats from Internet access;
- 8.2 No personal data should be sent over the Internet unless it is encrypted or otherwise secured;
- 8.3 Virus protection will be installed and updated regularly;
- 8.4 Personal storage devices such as USB memory sticks, MP3 players and digital cameras (SD cards) may not be brought into school without specific permission and a virus check. Any unauthorised items may be confiscated, placed in a secure area and returned to the user at the end of the school day.
- 8.5 Devices that are taken and used away from the school will be subject to regular scrutiny to ensure that malicious applications do not breach network security systems

9 How will e-mail be managed?

- 9.1 Communications with persons and organisations will be managed to ensure appropriate educational use and that the good name of the School is maintained

10 How will publishing on the Web be managed?

- 10.1 The CEO will have editorial responsibility to ensure that content is accurate and quality of presentation is maintained;
- 10.2 Web sites will comply with the School's guidelines for publications;
- 10.3 All material must be the author's own work, credit the sources used and state clearly the author's identity or status;
- 10.4 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;
- 10.5 Photographs published on the Web will not have full names attached and anonymity will be protected where necessary.

11 Social Media

- 11.1 Use of Social media sites such as Facebook and Twitter is discouraged within school hours as this exposes vulnerable students to risk.

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

11.2 Staff should not authorise friend or follow requests from learners.

11.3 For further guidance on the safe use of social media please refer to the Safeguarding Policy.

12 How will incidents be handled?

12.1 The management of the acceptable use of the Internet in school is achieved by:

- 12.1.1 Protection software installed on the network
- 12.1.2 Acceptable Use Policy adopted by the school
- 12.1.3 Staff will sign to say they have read the policy
- 12.1.4 A range of disciplinary procedures for infringements of the policy
- 12.1.5 Whenever a learner or staff member infringes the policy, the final decision on the level of sanction will be at the discretion of the School's management team

13 Infringements

13.1 Learners Category A infringements

- 13.1.1 Accessing non-educational sites during lessons
- 13.1.2 Unauthorised use of e-mail, live chat on sites or social media
- 13.1.3 Use of file sharing sites on school premises.
- 13.1.4 Transmission of commercial or advertising material

13.1.5 Sanctions:

- 13.1.5.1 Staff will discuss appropriate use of the Internet with the learner and the probable consequences of continued misuse. The learner's attention will be drawn to the '*Rules for Responsible Internet Use*' and the incident will be recorded in line with the whole school behaviour policy.

13.2 Learners Category B infringements

- 13.2.1 Continual access to non-educational sites during lessons after being warned
- 13.2.2 Unauthorised use of email, live chat on sites or social media after being warned

13.2.4 Sanctions:

- 13.2.4.1 The infringement will be brought to the attention to the designated member of staff who will telephone the learner's parents/ carers informing them of her/ his continued misuse of the Internet. The Consequences of

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

continued misuse will be made clear to all concerned. The learner's attention will be drawn to the '*Rules for Responsible Internet Use*' and the incident will be recorded in line with the whole school Behaviour policy

13.3 Learners Category C infringements

13.3.1 Accidentally accessing offensive material and not logging off or notifying a member of staff of it

13.3.2 Any purchasing or ordering of items over the internet

13.3.3 Sanctions:

13.3.3.1 The infringement will be brought to the attention of the Head of School or designated member of staff who will write to the learner's parents/ carers to inform them of her/ his continued misuse of the Internet and to request a meeting at which this behavior may be addressed.

13.3.3.2 The learner's attention will be drawn to the '*Rules for Responsible Internet Use*' and he/she will be placed on a temporary ban from using the PC in line with the whole school Behaviour Policy.

13.3.3.3 The learner's use of the Internet will be closely monitored for half a term. Future use will depend on an appropriate response to the imposed sanctions.

13.4 Learners Category D infringements

13.4.1 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, violent or indicating extremism

13.4.2 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988

13.4.3 Bringing the School or School name into disrepute

13.4.4 Deliberately corrupting or destroying others' data, violating privacy of others

13.4.5 Sanctions:

13.4.5.1 The infringement will be brought to the attention of the Head of School who will write to the learner's parents/ carers to inform them of her/ his

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

- continued misuse of the Internet and to request a meeting at which this behaviour may be addressed. The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and s/he will be placed on a ban, in line with the whole school Behaviour Response Code.
- 13.4.5.2 Future access to the Internet will be at the discretion of the Head of School.
- 13.4.5.3 It may be necessary for The Head Teacher or The Education Manager to refer the matter, as a Safeguarding Issue or make a referral to The Police in the case of suspicion of Radicalisation.

14 Staff

- 14.1 The following activities will be considered a breach of the School code of staff conduct and could result in disciplinary action.

- 14.1.1 Excessive use of Internet for personal activities not related to professional development
- 14.1.2 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, violent or indicating extremism
- 14.1.3 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018
- 14.1.4 Bringing the school name into disrepute
- 14.1.5 Befriending learners on personal social media accounts
- 14.1.6 Unauthorised use of computers as per the Computer Misuse Act 1990
- 14.1.7 Misuse of data as per the Data Protection Act 2018
- 14.1.8 Breaching the Copyright, Designs and Patents Act 1988

15 How will staff and learners be informed?

- 15.1 Rules for Internet access will be posted near computer systems.
- 15.2 The Acceptable Use Statement or Rules for Responsible Internet Use will be printed as posters
- 15.3 All staff will be provided with the e learning safe use policy, and its importance will be explained. The policy will be made available to parents on request
- 15.4 A module on responsible Internet use will be addressed in PSHE and citizenship.

16 Policy Links

- 16.1 This policy links with the following:
 - 16.1.1 Safeguarding Policy

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

- 16.1.2 Behaviour Policy
- 16.1.3 H & S policy
- 16.1.4 Data Protection Policy

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

Student Acceptable Use of IT Agreement

The school network has computers with Internet access to help our learning. These rules will keep us safe and help us to use the computers fairly.

- I will only use the computers on the school network with permission from an adult;
- I will only login with the username assigned to me;
- I will save all my work in my own user area on the H: drive;
- I will only access the websites as directed by my teacher;
- I will not access other people's files;
- I will not download files without an adults permission;
- I will use the computers for schoolwork and homework;
- I will not bring USB memory devices from outside school unless I have been given permission;
- I will only e-mail people I know, or those approved by my teacher;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand that this report would be confidential and would help protect other learners and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I understand that access to the Internet is for the purpose of learning;
- I will not use social networking sites;
- I will not attempt to bypass the school's filters;
- I will keep my password to myself.

Signed: _____ Date: _____
(Student)

Signed: _____ Date: _____
(Parent)

Signed: _____ Date: _____
(Head Teacher/Education Manager)

Date:	September 2019	E-Safety Policy (Norfolk)	Document N°	E10a
Version:	001		Written by:	M Norman
Review Date:	September 2020		Reviewed by:	M Norman

Staff Acceptable Use of IT Agreement

The rules below apply to all computers on the school network and to any portable IT or media devices that are the property of the school and are designated for use by individual members of staff. These rules are designed to ensure that a safe ICT environment is maintained for use by all staff and pupils and ensures that the security and integrity of data is preserved.

- I will comply with all aspects of the Ryes College's Code of conduct;
- I will undergo any necessary online ICT training;
- I will only use the computers on the school network for school related work;
- I will only login with the username assigned to me by IT support.
- I will save all my work in my own user area on the H: drive or in the school's shared area;
- I will only access appropriate websites for teaching and learning;
- I will not access other people's files;
- I will not download files;
- The email messages I send will be for business purposes only;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not attempt to bypass the school's filters.

Signed: _____ Date: _____
(Staff Member)

Signed: _____ Date: _____
(Line Manager)

Signed: _____ Date: _____
(Headteacher/Education Manager)