Castle Newnham School

TRADITIONAL VALUES, BRIGHT FUTURES, ONE JOURNEY

E-SAFETY

Policy

Governors' Committee:	Resource Management Committee
Adopted by the Governing Body on:	21 January 2021
Signed: (Chair of Committee)	
Signed: (Headteacher)	
Proposed date of review:	January 2023

A. RATIONALE

- The internet is an integral part of 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience. The purpose of internet use in school is to help raise educational standards, promote pupil achievement, teach pupils good internet practice, support the professional work of staff, and enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

- This policy has been developed to ensure that all adults at Castle Newnham School are working together to safeguard and promote the welfare of children and young people.

- This policy links to:

  - Safeguarding
  - Anti-Bullying
  - Staff code of conduct

B. AIM

i. To promote the safe and effective use of ICT to support learning and the smooth running of school systems;
ii. To identify simple ways in which e-safety issues can be reported to responsible adults.
iii. To provide a clear policy and guidelines to enable e-safety to be tackled effectively.
iv. To put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained through the use of ICT, whilst minimising any associated risks.
v. To minimise the potential risk of harm to pupils or staff in the following broad areas:
vi. Exposure to illegal, inappropriate or harmful material
vii. Subjection to harmful online interaction with other users
viii. Engagement in behaviour that increases the likelihood of, or causes, harm.

C. PRINCIPLES

i. All staff can recognise and are aware of e-safety issues with regular training and updates;
ii. E-safety is a priority across all areas of the school;
iii. E-Safety is a safeguarding issue as well as an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.
iv. The contribution of pupils, parents and the wider school community is valued and integrated.
v. The curriculum should ensure varied and regular opportunities to teach pupils explicitly about e-safety.

D. PROCESSES

ROLES AND RESPONSIBILITIES

1. The Federation Principal, senior leaders or in their absence, the Designated Child Protection Officer have the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care;

2. All members of the school staff have a role in ensuring safe and purposeful use of the internet and other ICT and are responsible for such both on the school site and off when supervising out-of-class activities. This role will be carried out during lessons where ICT is in use and in tutor sessions, other lessons as appropriate, assemblies and in informal meetings with pupils involving their safety and wellbeing.

USING THE INTERNET SAFELY TO ENHANCE LEARNING

i. Staff will be made aware of (through CPD and published guidance) and pupils will be educated in the safe use of the internet;

ii. Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the internet and digital communications;

iii. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation;

iv. Staff will endeavour to ensure that the use of internet derived materials by staff and by pupils complies with copyright law;

v. If staff or pupils discover an unsuitable site, it must be reported to an e-Safety (safeguarding) lead via any member of staff. The Federation Principal and designated e-safety (safeguarding) leads will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;

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

vii. All staff (both sites) and all pupils (North site only), upon joining the school, will be required to sign the respective Acceptable Use Agreement (Appendix 1 & 2).

USE OF EMAIL

i. Pupils in Secondary are allocated a school email address

ii. Pupils and staff should only use approved curriculum e-mail accounts (@castlenewnham.school);

iii. Pupils must be made aware of how they can report abuse and who they should report abuse to;

iv. Pupils will be told to report if they receive offensive or inappropriate e-mail;

v. In e-mail communication, pupils will be advised not reveal their personal details or those of others, or arrange to meet anyone without specific permission;

vi. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known;

vii. All staff users will include a signature giving their name, job title and the school contact details as per an agreed protocol;

viii. Staff must not use the school email system to promote activity outside of school (such as a business interest nor to arrange or discuss social activity unconnected with school business);

ix. The forwarding of chain letters is not permitted.

MANAGING INTERNET ACCESS AND INFORMATION SYSTEM SECURITY

i. The school ICT system security will be reviewed regularly with our ICT support provider;

ii. The Federation Principal and the designated member of staff for e-safety will receive reports of any concerns about internet or email usage and will act upon these accordingly;

iii. Virus protection will be installed and updated regularly.

PUBLISHED CONTENT AND THE SCHOOL WEB SITE

i. Staff or student personal contact information will not be published on the website or via social media. The contact details given online should be the school office;

ii. The Federation Principal or nominee will take overall editorial responsibility and ensure that published content is accurate, regularly updated and appropriate.

PUBLISHING PUPILS' IMAGES AND WORK

i. Photographs that include pupils will be selected carefully with due regard to requests for "no photographs" so that images of individual pupils cannot be misused;

ii. No photographs of pupils should be taken using staff's own devices;

iii. Pupils' full names will not be used in association with photographs of individuals on the website or in social media;

iv. Written permission, using the approved permission form, from parents or carers will be obtained before photographs of pupils or their work are published on the school website. This will be renewed annually.

SOCIAL NETWORKING AND PERSONAL PUBLISHING

i. Staff will be trained in the safe use of social networking sites, and will educate pupils in their safe use. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

ii. Pupils must be made aware of how they can report abuse using the facilities provided by social media sites and parents will be alerted where any misuse comes to light.

iii. Guidance to parents on the safe use of social media will be available on the school website;

iv. Guidance provided by the local authority or the police will be provided and updated via the school website;

v. Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future;

vi. Pupils will be advised through lessons in school and assemblies, be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils will be told to only invite known friends and deny access to others.

MANAGING EMERGING TECHNOLOGIES

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

ii. Any school mobile phone will be used only on trips for essential communication with the office or with parents;

iii. The sending of abusive or inappropriate text messages is forbidden in school and parents and the police will be involved as deemed necessary by senior staff;

iv. Senior staff are aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Pupils are not allowed to use mobile phones in school. They are advised to store them in the office if parents require them to have a phone before or after school. Pupil use of mobile phones on residential trips may be authorised or prohibited after consultation by the trip lead with a senior member of staff. This will be kept under review.

v. Mobile phones belonging to members of staff should not be visible in areas where pupils are present.

PROTECTING PERSONAL DATA

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

POLICY DECISIONS

Authorising Internet access

i. All staff, including temporary staff and volunteers as well as governors must read and sign the 'Acceptable Use Policy and Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use and must sign to say they will abide by its requirements;

ii. Parents/carers and pupils will be asked to sign and return an agreement form regarding acceptable use of ICT;

iii. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

ASSESSING RISKS

Castle Newnham will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school's network. The school will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken.

3. MONITORING, ASSESSMENT & EVALUATION

i. Information to assist with the monitoring of the policy will be collected in the following ways:
ii. Staff feedback
iii. Behaviour incidents and other logs
iv. Pupil and parent feedback
v. Regular meetings between the Federation Principal, network management provider and designated leads for e-safety (Safeguarding leads)
vi. Reports to governors
vii. Governor visits to challenge leaders on E-Safety arrangements

Appendix 1

Castle Newnham School

TRADITIONAL VALUES, BRIGHT FUTURES, ONE JOURNEY

ICT- PUPIL ACCEPTABLE USE AGREEMENT
Castle Newnham School

- I will only use a computer when supervised or instructed to by an adult.
- I will only use ICT in school for school purposes.
- I will not download or install software on school equipment.
- I will not use any personal hardware that could cause damage to school equipment.
- I will not tell other people my ICT passwords.
- I will only open email attachments from people I know, or that my teacher has approved.
- I will make sure that all ICT communications with pupils and adults are responsible, polite and sensible.
- I will be responsible for my behaviour when using the internet (this includes the resources I access and the language I use).
- I will not deliberately search for, download or send material that could be unpleasant or offensive. If I accidently come across such material I will report it immediately to my teacher.
- I will not give out any personal information such as my name, phone number or address.
- I know that my use of ICT can be checked and that my parent/carer can be contacted if a member of school staff is concerned about my e-Safety.
- I will not publish pictures of school peers without their permission.
- I understand that these rules are designed to keep me safe, and that if they are not followed school sanctions will be applied and my parent/carer may be contacted.

Name of pupil: .....Reg: .....

Signature of pupil:.....Date: .....

Appendix 2

IT ACCEPTABLE USE POLICY FOR ALL ADULTS WORKING AT CASTLE NEWNHAM

The school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring.

All adults using ICT equipment within the school must ensure that they have read and abide by the Acceptable Use Policy. If they are found to have contravened any of the requirements they may face disciplinary action.

The school's ICT systems and network should be used primarily for school purposes but **occasional** personal use is permitted during 'non-contact' time and out of school hours. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

ICT equipment

- I will not give anyone access to my login name or password (unless authorised by the Head Teacher).
- I will not attempt to introduce any unlicensed applications.
- I will not corrupt, interfere with or destroy any other user's information.
- I will not release any personal details of any colleague or pupil over the internet, particularly on social networking sites such as 'Facebook' or 'Twitter'.
- I will not use the school internet access for business, profit, advertising or political purposes.
- I will not leave my account open at the end of a session.
- I will not engage in any activity which might compromise the security of the school network.
- I will not install, attempt to install or store programs of any type without permission of a member of the Senior Leadership Team.

E-mail

- E-mails should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny.
- I will not include offensive or abusive language in my messages or any language which could be considered defamatory, obscene or menacing.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- I will make sure that nothing in messages could be interpreted as libellous.
- I will not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
- I will not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.
- I will never open attachments to e-mails unless they come from someone I know and trust.

Internet

- I will watch for accidental access to inappropriate materials and report any offending site to the ICT Subject Leader/ICT technical support provider/Data Manager and Head Teacher so that action can be taken.

- I will check copyright before publishing any work and ensure that any necessary permission is obtained.
- I will ensure that the school's photo policy is strictly adhered to.
- I will report any breaches of the e-Safety policy to the ICT Subject Leader/ Head Teacher/Data Manager.
- I will only use social media to promote the school/school activities and not to pass on unsuitable information or images/details of pupils or staff.

Mobile Phones

- I will not use my mobile phone during lesson or registration times. If required to do so, due to special circumstances, I will get permission from a member of SLT.

Name: _____ (Please use block capitals)

Signature: _____ **Date:** _____