

Acceptable Computer &

Internet Use Policy

September 2021

Review date: September 2022

|  |
| --- |
| It is the responsibility of all staff to ensure that this policy is adhered to and that pupils are made aware of the potential risks and benefits associated with computer and internet use. |

**Security and Data Management**

In line with requirements of the General Data Protection Regulations (2018) sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data must be:

* Accurate
* Secure
* Fairly and lawfully processed
* Processed for limited purposes
* Processed in accordance with the data subject’s rights
* Adequate and relevant and not excessive
* Kept no longer than is necessary
* Only transferred to others with adequate protection

All data will be kept secure and staff informed of what they can or cannot do with data through the Acceptable Use Policy and Data Protection Policy.

**Use of Mobile Devices**

* Pupil’s mobile devices are handed in when they arrive at school and placed in their individual locker.
* Staff must keep their own personal mobile devices in either staff lockers or locked in the staff room.
* Staff must not use their own personal mobile phones during working hours unless it is an emergency or have discussed previously with the Headteacher.
* Staff must only use school mobile phones whilst in the building or on school related business or visits.

**Use of Digital Media**

All parents/carers are asked for permission to take pictures of pupils during their admissions meeting. Staff must follow the Lancashire County Council guidelines regarding the taking of photographs and must not use personal devices for taking or storage.

**Communication Technologies**

**Email**

* Staff can access their school email via Lancashire Grid for Learning or Office 365.
* Staff must not use personal email accounts during school hours or for school activities.
* Pupils must use school email accounts where applicable, they cannot access personal email accounts due to filtering systems in place.
* Should staff need to email pupils work they must use the pupils school email account only.
* Any confidential information and or files that need to be transmitted will be done so using a secure and encrypted email.

 **Social Networks/Social Media**

* Pupils and staff must not access social networking or media sites during working hours of the school day on personal devices or school computers.
* Staff are aware of Lancashire County Council guidelines as regards communicating with pupils via social networking/media sites via school’s Social Networking Sites and Social Media Policy.

 **School website**

* Chadwick High has its own school website which contains all statutory information.
* No pupil full names will be used on the school website particularly in association with photographs.
* Written permission from parents or carers will be obtained at admissions as regards the use of photographs of pupils on the school website.

**Infrastructure and Technology**

* Pupils are supervised when accessing school equipment and online materials.
* Pupils have their own logins and have restricted access to the school network.
* All staff have secure usernames and passwords and are restricted to areas of the network according to their areas of responsibility.
* Staff passwords are automatically changed on a regular basis.
* All software has the necessary license.
* Equipment and software is regularly updated with anti-virus protection and audited.
* If staff require a website to be blocked/unblocked then this must be reported to the Office to enable corrective action to be taken.

**Dealing with Incidents**

* Staff are made aware of the E-Safety policy and procedures via staff training sessions.
* An incident log is completed to record and monitor offences. This will be audited on a termly basis by the SLT (see Appendix 1). All staff are responsible for dealing with any E-Safety Incidents and informing the Headteacher and DSL.
* **Illegal Offences**: any suspected illegal material or activity will be brought to the immediate attention of the Headteacher who will refer it on to external agencies as appropriate eg Police, CEOP. The school will not personally investigate, interfere with or share evidence as staff may be inadvertently committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

**Examples of illegal offences are**:

* Accessing child sexual abuse images
* Accessing non–photographic child sexual abuse images
* Accessing criminally obscene adult content
* Accessing websites or materials which incite racial hatred, homophobia,

religious hatred

* Pupils and Parents are informed of and sign the Acceptable Computer and Internet Use Agreement during the admissions meeting.
* All staff are aware of the different types of E-Safety incident and how to respond appropriately.

|  |  |
| --- | --- |
| Incident | Procedure and Sanctions |
| Accidental access to inappropriate materials | Minimise the webpage/turn the monitor offSpeak to the pupil concernedRecord the incident in the LogPersistent “accidental offenders” may need further disciplinary action |

|  |  |
| --- | --- |
| Incident | Procedure and Sanctions |
| Using other peoples log ins and passwords maliciouslyDeliberate searching for inappropriate materialsBringing inappropriate electronic files from homeUsing chat and forums in an inappropriate way | Inform SLT/DSLEnter the incident details in the LogDiscuss with the pupils concernedMore serious or persistent offenders will be dealt with via the Behaviour PolicyRaise awareness with the individual pupil/group of pupils as regards the E-Safety Policy, Acceptable Use Policy and how to keep safe online |

**E-Safety across the Curriculum**

* It is vital that pupils are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others E-Safety. This is done via ICT and PSHE lessons. Additional E-Safety focus will be made during the National E-Safety Awareness Week.
* All staff are responsible for displaying the Safe Internet Use Guidelines within their classrooms/teaching spaces
* Pupils need to be made aware of the three main areas of E-Safety.

|  |  |
| --- | --- |
| Area of Risk | Example of Risk |
| Pupils need to be taught that not all content is appropriate or from a reliable source | Exposure to inappropriate content including online pornography, ignoring age ratings in games, substance abuse, lifestyle websites: self-harm, suicide websitesHate sites/chat rooms |
| Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies | GroomingCyberbullying in all formsIdentity theft and sharing passwords |

|  |  |
| --- | --- |
| Area of Risk | Example of Risk |
| Pupils need to be made aware that their personal online behaviour can increase the likelihood of or cause harm to themselves and others | GroomingCyberbullying in all formsIdentity theft and sharing passwords |

**E-Safety – Raising Awareness**

* E-Safety training is delivered annually to all staff and is discussed in Staff meetings on a regular basis as part of the Safeguarding agenda item. All members of staff are given a copy of this policy as part of their Staff Handbook.
* New members of staff to Chadwick High School are given information regarding the E-Safety policy.
* The Governing Body receive annual training around E-Safety from the DSL.
* Parents/Carers are made aware of the E-Safety Policy via the website and at admissions meetings.

**Teaching and Learning**

* The purpose of Internet Use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems.
* Chadwick High School’s internet access will be designed expressly for pupils use and will include filtering appropriate to the age of the pupils.
* Pupils will be taught in ICT lessons and via the PSHE curriculum what Internet use is acceptable and what is not and given clear guidance and objectives as regards its use.
* Pupils will be able to access the Internet during a variety of lessons and subject areas. Staff are responsible for ensuring effective and appropriate Internet use during their lessons.
* Chadwick High School will provide opportunities for pupils to develop internet skills such as knowledge location and retrieval, evaluation, access to worldwide educational resources as part of their overall learning experience

**Managing Internet Access**

* If staff or pupils discover unsuitable sites the URL (address) and contents will be reported to the HT and school office, this information with then be passed onto the IT/Internet Service Provider.
* Chadwick High School will endeavour to ensure that the use of Internet derived materials by staff and pupil’s compiles with copyright law.
* Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
* Pupils will be taught what is and is not acceptable and given clear objectives and guidance for Internet use for both school and home use.
* Staff will guide pupils in online activities as appropriate which support the learning outcomes and matched to the pupils’ age and maturity.
* Pupils will be monitored at all times when accessing the Internet by a member of staff.
* Any internet misuse must be recorded and the Headteacher/DSL informed.
* If pupils use social media to bring the school into disrepute or criticise staff it will be dealt with in line with the School Behaviour Policy and may be reported to the Police.
* Staff should read the guidance in the Policy on the Use of Social Networking Sites and other Forms of Social Media as regards their own personal use of social media.
* Newsgroups and social networking sites will be blocked.
* Pupils may only access school email accounts on the school system.
* Chadwick High Schools IT systems will be reviewed regularly with regards to security.
* Anti-Virus Protection will be installed and updated regularly.
* SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate effective and reasonable.
* The Filtering System is provided by BTLS.
* Emerging technologies will be examined for educational benefits and a risk assessment carried out before use in school is allowed.
* Mobile phones will not be used during the formal school day by pupils or staff.

**Policy Decisions**

* Parents/carers will be informed of the E-safety Policy on admission and will be asked to sign the consent form.
* Pupils will be asked to sign an acceptable use of Internet/Computer in their ICT lessons/at their Admissions Meeting.
* Staff will sign the Acceptable Use of the Internet/Computer form annually.
* The school will take all reasonable precautions to ensure that users access only appropriate materials. However, due to the international scale and linked nature of Internet content it is not possible to guarantee that unsuitable materials will never appear on a school computer
* Methods to identify, assess and minimise risks will be reviewed regularly.
* Complaints of Internet misuse will be dealt with in the first instance by all members of staff and reported to the Headteacher/DSL who will then deal with it further as appropriate.
* Any complaint about staff misuse must be referred to the Headteacher.
* Complaints of a Child Protection/Safeguarding nature must be immediately brought to the attention of the DSL and dealt with in accordance with Chadwick High School Child Protection/Safeguarding Policy.

**Communications Policy**

* E-Safety Rules will be posted near all computers.
* All staff will give pupils regular reminders as regards E-Safety.
* Pupils will be informed that Internet use will be monitored.
* All staff must accept the terms of the Responsible Internet Use Policy before using any Internet Resource in school.
* All staff will be given a copy of the E-Safety Policy annually.
* All staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential and expected.
* Internet issues will be handled sensitively to inform parents/carers without undue alarm.
* Parents/Carers attention will be drawn to the E-Safety Policy at Admissions and via the School website.



**Acceptable Computer and Internet Use Policy**

**Pupil Agreement**

**Using the Computers:**

* I will only access the computer system with the login and password I have been given
* I will not access other person’s files or use their login details
* I will not use CDs, DVDs, USBs from outside of school and try to use them on the school computers without permission
* I will use all equipment respectfully
* I will log off when I have finished using the computer

 **Using the Internet:**

* I will ask permission from a member of staff before using the internet
* I will report any unpleasant material to a member of staff immediately because this will help protect other pupils and myself
* I understand that the school may check my computer files and may monitor the internet sites I visit
* I will not complete and send forms without permission from a member of staff
* I will not give my full name, my home address or telephone number when completing online forms until I have checked this with a member of staff
* I will use the internet for educational and research purpose only
* I will not access Social Media Sites whilst in school

 **Using E-mail**

* I will not access personal email accounts whilst in school
* I will only use email accounts which are set up in controlled settings for the purposes of classroom practices
* I will not give out any personal details to any Third Parties

I understand and agree to follow this policy and understand that if I fail to comply with these rules it could result in my being unable to use/access the school computers and internet system.

Signed…………………………………………………………… Date………………………………



**Acceptable Computer and Internet Use Policy**

**Staff Agreement**

**Using the Computers:**

* I will only access the computer system with the login and password I have been given
* I will not access other people’s files or use their login details
* I will use all equipment respectfully
* I will log off when I have finished using the computers

**Using the Internet:**

* I will report any unpleasant material immediately to the School Business Manager
* I understand that the School and the ICT technicians may check my computer files and may monitor the internet sites I access
* I will not access personal information (bank accounts etc.) whilst in school as details can be recovered by Third Parties
* I will not open any unknown or suspicious attachments or executables (programme files)
* I will not access Social Networking or Media Sites on school computers or during working hours

**Data Transfer:**

* I will not access personal email accounts whilst in school to send confidential emails
* I will use email or cloud based technology for transfer of work documents
* I will not use portable hard drives, USBs, CDs, DVDs without school authorisation
* I will only use encrypted USBs to transport confidential information with school authorisation
* I will follow all Data Protection and General Data Protection Regulations

I understand and agree to adhere to this policy and the points outlined above.

Signed……………………………………………………… Date…………………………