Congleton High School
E Safety Policy
2018/2019

Achieving Success Together

Approved by the CHS LGB 5th July 2018

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Congleton High School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Congleton High School
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for Congleton High School can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope
This policy applies to all members of Congleton High School (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Congleton High School.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This includes incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to students or staff of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see Congleton High School Behaviour Policy).

The school will deal with such incidents within this policy and the behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
CEO and Head of School	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security • To ensure the school uses an industry standard web filtering system. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures

E-Safety Co-ordinator / Designated Safeguarding Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	•
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors / E-safety Governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
ICT Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly

Network Manager/technician	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that virus protection is kept up to date • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure that any misuse / attempted misuse of the network is reported to the E- Safety Co-ordinator for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures

Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities) • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. personal email, text, mobile phones etc.
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-safety policies

Parents/Carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website/ on-line Student Portal in accordance with the school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication:
The policy will be communicated to staff/students/community in the following ways:

- Policy will be posted on the school website.
- Policy to be part of school induction pack for new staff and posted on BlueSky.
- Acceptable use agreements will be discussed with students at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in student and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.
  Congleton High School cannot accept liability for material accessed, or any consequences of Internet access.
- Staff and students are given information about infringements in use and possible consequences. Consequences may include:
    - Meeting with the Tutor/Guidance Team Leader / e-Safety Coordinator / Head of School
    - Sanctions in line with the Discipline for Learning Policy
    - 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];
    - Referral to the LA / LSCB / Police.

- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is also referred to the e-Safety Coordinator.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

- Complaints related to child protection are dealt with in accordance with our Safeguarding Policy

Review and Monitoring

The e-safety policy is referenced from within other school policies: ICT Curriculum Area policy, Safeguarding policy, Behaviour policy, Anti-Bullying policy and in the School Development Plan,

The school has an e-safety coordinator who will be responsible for document ownership, review and updates.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as Parents in Partnership. All amendments to the school e-Safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Student e-Safety curriculum

This school

- Has a clear, e-safety education programme as part of the ICT curriculum. This covers a range of skills and behaviours including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign in their Planner
- Ensures staff will model safe and responsible behaviour in their own use of technology during

lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around

plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-Safety policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear. Parents are expected to sign the Acceptable Use Agreement in the student planner in respect of their child.
    - Information leaflets; in school newsletters; on the school web site;
    - Demonstrations, practical sessions held at school;
    - Suggestions for safe Internet use at home;
    - Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

At Congleton High School, all users:

- are responsible for using the school ICT systems in accordance with the Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's s-Safety policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for students to use the Internet, as well as other technologies, as part of

the e-safety acceptable use agreement form at time of their child's entry to the school

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

At Congleton High School:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's disciplinary processes.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline and CEOP) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and reported to the Senior Leadership Team, Governors /the LA / LSCB
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

  This school:

  - Ensures the network is healthy through use of anti-virus software and the network is set-up so staff and students cannot download executable files;
  - Has blocked Student access to music download or shopping sites – except those approved for educational purposes.
  - Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
  - Provides advice and information on reporting offensive materials, abuse/ bullying etc to all students, staff and parents
  - Immediately refers any material we suspect is illegal to the appropriate authorities such as the Police, CEOP, the LA.

- **Network management (user access, backup)**

  This school

  - Uses individual, audited log-ins for all users
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Ensures the Systems Administrator / network manager is up-to-date with all services and policies
  - Storage of all data within the school will conform to GDPR

To ensure the network is used safely, Congleton High School:

- Ensures staff read and sign that they have understood the school's ICT Acceptable Use Policy. Following this, they are set-up with Internet, email access and network access.
- Online access to the service is through a unique username and complex password.
- Staff access to the schools' management information system (Progresso) is controlled through a separate password for data security purposes;
- We provide students with an individual network log-in username, they are also expected to use a personal password;
- All students have their own unique username and password which gives them access to the Internet, the VLE and their own school email account;
- All students are expected to read and sign the ICT Acceptable Use Policy in their school planner. Parents are also expected to counter sign the Policy

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find. ;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords to access the school system
- Staff are automatically required to change their passwords on the management information system (Progresso) and on the school network every 90 days.

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

Students:

- Are introduced to, and use e-mail as part of the ICT program of study
- Are expected to communicate with staff using their school email not their personal email
- Are expected to comply with the Student ICT Acceptable Use Policy when using their email account

Staff:

- Must use their school email address for all school related communication in line with the Staff Acceptable Use Policy
- Access in school to external personal e mail accounts may be blocked

- Never use email to openly transfer staff or pupil personal data. Personal data must only be transferred in encrypted form and marked as confidential in line with the Staff ICT Acceptable Use Policy.
- Staff know that e-mail sent to an external organisation must be written carefully and in the same way as a letter written on school headed paper.

School website

- The Principal/Head of School takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authoriser.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. enquiries@Congletonhigh.com
- Individual staff contact is done via the web site and through a staff contact form, individual email addresses are not displayed
- Photographs published on the web do not have full names attached;
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

VLE (LIFE)

- Uploading of information on the schools' VLE is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools VLE will only be accessible by members of the school community;

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' email system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / students, parents / Carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

***5*. Data security: Management Information System access and Data transfer**

Strategic and operational practices

At Congleton High School:

- The Executive Principal is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in on a central record and in Progresso
- We ensure ALL the following school stakeholders are made aware of the Acceptable Use Agreement. On Bluesky and the website
    - staff,
    - governors,
    - pupils
    - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs
- We require staff to log-out of systems when leaving their computer and to lock their screens when they are away from the computer for short periods
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area
- All servers are in lockable locations and managed by DBS-checked staff.
- We comply with the directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones and personally-owned mobile devices are brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school

.

- Student mobile phones which are brought into school must be used in accordance with the Mobile Phone/ Personal Music Player Acceptable Use Policy.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

Digital images and video

At Congleton High School:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Person responsible for the Policy:	Mrs G. Taylor
Date Approved:	
Signed:	
Date for Review:	April 2018