CULCHETH HIGH SCHOOL

› THE BEST THAT WE CAN BE

E-SAFETY POLICY

Reviewer: S. Piggott

Reviewed: August 2016

RATIFIED BY THE GOVERNING BODY
19/10/16

› RESPECT
› HONESTY
› EXCELLENCE

CONTENTS

Development / Monitoring / Review of this Policy

This E-Safety policy has been developed by a working group made up of:

- *Headteacher / Senior Leaders C. Hunt, N. Brearley*
- *E-Safety Manager S.Piggott*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors, Colin Grime*

Schedule for Development / Monitoring / Review

This E-Safety policy was approved by the Governing Body on*:*	October 2016
The implementation of this E-Safety policy will be monitored by the Child Protection Officer and Governing Body:	E-Safety Manager
Monitoring will take place at regular intervals:	At Line Management Meetings
The *Governing Body Committee* will receive a report on the implementation of the E-Safety policy generated by the monitoring group (which will include anonymous details of e- safety incidents) at regular intervals:	At Governing body meetings
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next anticipated review date will be:	October 2017
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	Cheshire Police

The school will monitor the impact of the policy using:

- Logs of reported incidents, including files opened, saved, deleted and printed
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
- students
- parents / carers
- staff

Scope

This E-Safety policy applies to all members of the Culcheth High School community (including staff, temporary staff, Initial Teacher Training staff, students, volunteers, parents/carers, visitors, community users, leisure users and Governors) who have access to and are users of school network and management systems both in and out of school. This includes all web based Culcheth High School branded websites, intranets, social media accounts and marketing areas.

The Education and Inspections Act 2006 empowers Head teachers, 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 is pertinent to incidents of cyberbullying, or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated 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.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals within Culcheth High School:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors 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 (as part of the Child Protection Governor role). The role of the E-Safety Governor will include:
    - regular meetings with the E-Safety Manager
    - regular monitoring of E-Safety incident logs
    - regular monitoring of filtering / change control logs
    - reporting to relevant Governors / committees

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Manager.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Manager and other relevant staff receive suitable training.

- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Manager.

E-Safety Manager is responsible for ensuring:

- that they are leader of the E-Safety committee.
- takes day to day responsibility for E-Safety issues and has a sole role in establishing and reviewing the school E-Safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e- safety incident taking place both inside and outside of school.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises and leads school technical staff with reporting and monitoring.
- receives and produces reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/ change control logs.
- attends relevant meetings / committees of Governors.
- reports regularly to Senior Leadership Team.

The ICT Support department is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack to the best of their knowledge.
- that Culcheth High School meets required E-Safety technical requirements and any other relevant body E- Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- work closely with filtering and security provider to ensure the latest filtering and protection methods are applied to the firewall and filtering software.
- that they keep up to date with E-Safety technical information in order to effectively carry out their e- safety role and to inform and update others as relevant.
- that the use of the network / internet / Google and clouds services / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; E-Safety Coordinator for investigation / action / sanction.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety policies and procedures and the current and latest E-Safety practices.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Manager for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the E-Safety and acceptable use policies.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor network activity in lessons, extra-curricular and extended school activities using school approved systems.
- in lessons students are guided with the use of the Internet by the Teachers/Support teacher within the class to suitable pages and safe search results.
- take personal responsibility for their professional development in this area.

Child Protection / Safeguarding Designated Person

Should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding 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
- extremism
- self-harm
- sexting

E-Safety Group

The E-Safety Group (Stuart Piggott – E-Safety Manager, Nicola Brearley Safeguarding SLT, Carlo Mullen, Senior ICT Technician, John Morris Senior ICT Technician and Joanna Shaw, PSHE Co-Ordinator, Colin Grimes, E-Safety Governor) provides a consultative group that has wide representation from the Culcheth High School community, with responsibility for issues regarding E-Safety and the monitoring the E-Safety policy including the impact of initiatives.
The group/E-Safety Manager will also be responsible for regular reporting to the Governing Body.

Members of the E-Safety Group will assist the E-Safety Manager (or other relevant person, as above) with:

- the production / review / monitoring of the school E-Safety policy / documents.
- the production / review / monitoring of the school filtering policy.
- mapping and reviewing the E-Safety curricular provision – ensuring relevance within the classroom environment.
- monitoring network / internet / incident logs.
- consulting stakeholders – including parents / carers and the students / pupils about the E-Safety provision.

Students:

- are responsible for using Culcheth High School's digital technology systems in accordance with the Student Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so using school approved systems
- will be expected to know and understand policies on the use of mobile/tablet devices/digital cameras/Smart Phones.
  They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should 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.
- understand the E-Safety implications of taking and sharing personal data on social media or via the internet in general.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, local e- safety campaigns / literature and particularly a wealth of information on the school website available at all times. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website/ Google sites and social media pages.
- their children's personal devices in the school (where this is allowed) and fully understand the rules around the use of personal devices within school
- modelling appropriate uses of new and emerging technology.
- liaising with school if they suspect, or have identified, that their Child is conducting risky/hateful/ inappropriate behaviour online.

Community/Leisure User Responsibilities

Community/Leisure Users who access the school network or its affiliated systems as part of Extended School provision will be expected to sign the Staff Acceptable Use Policy before being provided the access to the network.

E-Safety Education

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students at Culcheth High School to take a responsible approach. The education of students in E-Safety is therefore an essential part of the school's e- safety approach and provision. Children and young people need the help and support of the school to recognise and avoid e- safety risks and build their resilience and realise the risks a lack of relevant E-Safety education brings.

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-Safety curriculum should be provided as part of Computing (with the involvement of PHSE/ other lessons) and should be regularly revisited.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities with real life examples where possible.
- Students should be taught in all lessons to be critically aware of the materials/ content they access on-line.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use not only at Culcheth High School but at home and in their general life.
- Staff should act as in an advisory capacity in their use of digital technologies the internet, social media and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites pre checked by Teaching staff and are fit for purpose and suitable for the Year group they are Teaching.
- Where students are allowed to search the internet, staff should be vigilant in monitoring the content of all websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination, extremism, sexting, hatred etc) that would normally result in internet searches being blocked. In such a situation, firstly staff are advised to find the relevant information on another site but if this is not possible staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Education – parents / carers

Parents play an essential role in the education of their children and in the monitoring/ regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet/social media and may need advice on how to deal with a situation.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters
- Comprehensive information the school website
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g.

http://culchethhigh.org.uk/parental/

www.saferinternet.org.uk/

http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Staff Teaching and Support

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the appraisal / performance development process.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- The E-Safety Manager (or other nominated person) will receive regular updates through attendance at external training if available.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

Training – Governors

Governors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / E-Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Education – The Wider Community

Culcheth High School can provide opportunities for local community groups / members of the community to gain from the school's E-Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety.
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide E-Safety information for the wider community.

Technical and Cloud Based Systems

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- Culcheth High School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and development including audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted via door locks and keypad control.
- All users will have clearly defined and relevant access rights to school technical systems and devices.
- The ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (such as child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the local authority filtering lists. Content lists are regularly updated and internet use is logged and regularly monitored. Culcheth High also have a robust and secure onsite Firewall system which can provide a various comprehensive lists of banned and enabled websites, this is differentiated between staff, students Year group dependant level filtering both on the wired and wireless infrastructure.
- The school ICT Support staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident /security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, VOIP phone system, wireless networks, work stations, mobile devices and cloud based systems such as Google and the website from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems and the access levels they are entitled to.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) can use Culcheth High school devices away from school premises.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices with the exception of Staff laptop’s, this is covered in the CHS Staff Laptop Loan Agreement.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. School data may be taken off site in a secured manor, encrypted devices are recommended.

- Social Media particularly through school Twitter approved school accounts is closely monitored and only available for staff to use and comment on.
- The school use of Cloud based technology is closely monitored and all emails/ communications with students is reported and auditable.
- Data that is present on Cloud based systems should be treated exactly the same as data onsite that is highly sensitive and needs to be kept very secure, careful consideration should be taken when offering to share personal data across Cloud systems.
- Cloud data is still the property of Culcheth High School, while it doesn't sit on the physical school premises it is to be treated in exactly the same manner as the data which resides on the physical site.

Filtering and the Internet

The filtering of internet content provides an essential means of preventing users from accessing material that is illegal or is inappropriate in an educational context. Culcheth High School's internet provision is provided by Warrington Borough Council provided by The Network People/ Fortigate/Fortinet

Fortigate/Fortinet are members of the Internet Watch Foundation (IWF) and block access to illegal Child Abuse Images and Content (CAIC).

The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web change on a daily basis and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for E-Safety and acceptable use. At Culcheth High School we have a multi-stage filtering system to manage the associated risks and to provide preventative measures, which are relevant to the situation in this school.

Internet access is filtered for all users, Key Stage 3 and Key Stage 4 are customised to allow students more access when necessary. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are updated daily and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school has differentiated user level filtering hardware firewall through the use of Sophos Unified Threat Management suite.
- Culcheth High have 2 processes of filtering, one option from the local authority and one locally set Unified Threat Management system. There is no option of avoidance of these filters using the CHS wired or wireless system.
- Filtering or bypassing of particular web pages can be requested by Teaching staff for educational purposes and reviewed by the ICT Support team.
- Filtering services **cannot** be turned off completely by request.

- Any mobile connections connecting to Culcheth High School will fall under the same standards as the main school regarding internet filtering with no exceptions.
- Any filtering issues should be reported immediately to the filtering provider.

Keyword filtering

In May 2016 the Government issued the statutory Guidance for "Keeping children safe in education" within this under "Annex C: Online Safety it expresses the need for appropriate Filtering and Monitoring. In accordance with the guidance from the UK Safer Internet Centre Culcheth High School incorporate a comprehensive piece of software (provided by Impero Solutions Ltd) which audits all devices and users at Culcheth High School, all usage is tracked from printing to deleting files, login attempts, and computer usage.

Impero Solutions are members of the Internet Watch Foundation (IWF) and block access to illegal Child Abuse Images and Content (CAIC).

Further to this all site users are suspect to Impero's keyword search, if a user breaches a keyword search a violation is allocated to that user and information such as time/date, which user and on which device is kept and a screenshot taken of the user's screen automatically and stored in a secure database only available to the E-Safety representatives, the information is stored until the user leaves the school, a breakdown of the categories Culcheth High school audit keywords is below:

Keyword category	Keywords within category
Adult Content	216
Bullying & Trolling	386
Drugs	3
Eating Disorders	122
Extremism	501
Gambling	3
Grooming	82
Hacking	7
Homophobic Language	232
Miscellaneous	6
Porn	18
Racism	21
Racist Language	99
Self-Harm	68
Sexting	39
Suicide	18
Violence	18

The system can deliver “false positives” and not all keywords accurately describe a user’s intended searches.

- The E-Safety Manager enforces and defines the search criteria and has a full operating knowledge of the software it uses and functions.
- The ICT Support ensure Impero is operational on a daily bases and have knowledge of its E-Safety uses.
- Qualified teaching staff may use Impero as classroom intervention tool but cannot see the keyword database entries.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons			X					X
Use of mobile phones in social time	X							X
Taking photos on mobile phones / cameras			X				X	
Use of other mobile devices e.g. tablets, gaming devices			X				X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails								X
Use of messaging apps			X					X
Use of social media			X					X
Use of blogs			X				X	

When using communication technologies, the school considers the following as good practice:

- The official Culcheth High School Google email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the class teacher – in the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

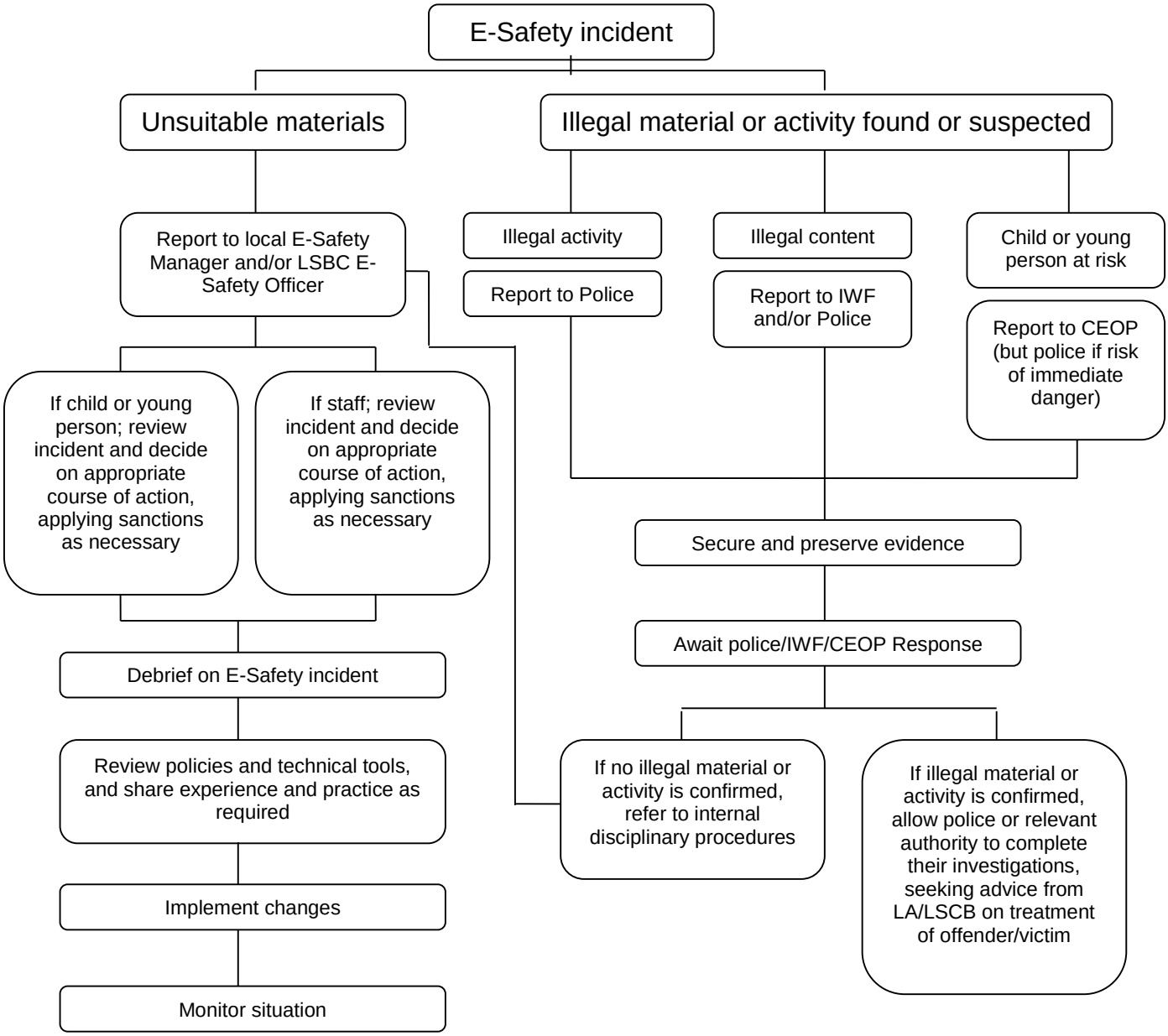
- Any digital communication between staff and pupils or parents / carers (Gmail, chat, Google Classroom etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

Passwords

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

- All users will be provided with a username and secure 8-digit password by the ICT Support department who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The secure "administrator" passwords for Culcheth High School ICT infrastructure used by the ICT Support Team must be available for a nominated Senior leader or directly to the Headteacher upon request and held in a secure place (server room).
- Passwords for new users, and replacement passwords for existing users will be allocated by ICT Support Team. Any changes carried out must be notified to this team immediately.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The level of security required may vary for staff and student / pupil accounts and the sensitive nature of any data accessed through that account).
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user, this may involve an identity check using SIMS.
- Where possible passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Students will be taught the importance of password security.

Responding to Incidents of Misuse



Glossary of Terms:

- LA: Local Authority
- LSBC: Local Safeguarding Children Board
- IWF: Internet Watch Foundation
- CEOP: Child Exploitation and Online Protection Centre

Other Incidents

It is hoped that all member of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps this procedure should be followed:

- Have more than one member of child protection staff / involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer(s) that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer(s) for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet/Wi-Fi access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation, Culcheth High school's current safeguarding software provides this.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour.
  - the sending of obscene materials to a child.
  - adult material which potentially breaches the Obscene Publications Act.
  - criminally racist material.
  - Extremism or hatred.
  - Radicalism.
  - other criminal conduct, activity or materials.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed literature should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. The nature of all of these incidents will vary, in light of this sanctions and actions will be dealt with on ad individual case by case basis.

E-Safety Incident Reporting Form

If you wish to report an E-Safety Incident, please use the form below and return to the E-Safety Team

E-Safety Incident Report Form

This form should be kept on file and a copy emailed to Culcheth High Schools e-safety officer sp@culchethhigh.org.uk

Date Incident Occurred:

Time:

Room:

Name of person reporting incident:

Name of students/persons involved:

Year/Form:

Details of incident

Where did the incident occur?
□ In school □ Outside school

Who was involved in the incident?
□ Child/young person Staff member Other (please specify)

Type of incident:
□ Bullying or harassment (cyber bullying
□ Deliberately bypassing security or access
□ Hacking or virus propagation
□ Racist, sexist, homophobic religious hate material
□ Terrorist material
□ Drug/bomb making material
□ Child abuse images
□ On-line gambling
□ Soft core pornographic material
□ Illegal hard core pornographic material
□ Other (please specify)

Description of incident

1

STUDENT – ACCEPTABLE USE GUIDELINES

Rationale

This Acceptable Use Policy is intended to ensure:

- that our students will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use
- that the school network and users are protected from accidental or deliberate misuse that could put the security of the network and users at risk

The school will endeavour to ensure that students will have the best possible access to ICT, Technology and cloud based learning environments to enhance their learning and will, in return, expect the students to agree to be responsible users.

Student Acceptable Use Policy Agreement

I understand that I must use school network (school network definitions are listed below, please read these before agreeing to this policy) in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the network and other users.

For my own personal safety:

- I will take responsibility for my personal security in relation to the use of all digital technologies
- I understand that the school will monitor my use on all school systems both inside and outside of school
- I will not share my network username and password with anyone
- I will not use any other person's network username and password
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when online including my name, address, location or any other personal details if I do not know them
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online

I understand that everyone has equal rights to use digital technology as a resource and:

- I understand that the school network is primarily intended for educational use and that I will not use the network for personal or recreational use
- I will not use the school network for online gaming, online gambling, Internet shopping, file sharing, or video broadcasting, I must report any websites that give me these features to a teacher immediately

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
- I will not take, amend, alter or distribute images of anyone

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand that the school reserves the right to monitor my use of the school network and all other school systems inside and outside of school
- I understand that the school will take steps set out in the E-Safety Policy if I choose to misuse the school network
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not download or upload from the Internet unless instructed to by a teacher
- I will not download executable files from the Internet, nor will I install executable files onto the school network from a removable storage device
- I will use removable storage devices (i.e. USB Memory Sticks) only for school use
- I will take every precaution to ensure that any removable storage device that I use is free from viruses
- I will immediately report any damage to school equipment or faults involving equipment or software, however this may have happened
- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings
- I will not access or use chat and social networking sites

When using the Internet for research, I recognise that:

- I will ensure that I have permission to use the original work of others in my own work
- I understand what Plagiarism means and the consequences if I copy work
- Where work is protected by copyright, I will not try to download copies
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour this includes outside of school and on social media. When I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police

School network definitions

For clarity listed below is what Culcheth High School class as “The School Network”

- Computer in ICT suites, normal classroom PC’s, Teaching Wall PC’s, iMac’s
- Mobile devices, iPads, iPods, Netbooks, tablets, Google Chromebooks, Macbooks, Apple TV’s, Spelling devices
- Wireless connections, inside of school and in the leisure areas such as the gym
- Google Apps for Education, Office 365, MyMaths, Maths Watch, Alfiesoft software, any school software which has be accessed in school or at home any software you login into from Culcheth High School

Please complete the sections at the bottom to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school network.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school network.

I have read and understand the above and agree to follow these guidelines when:

- I use the school network
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school and accessing school learning systems such as Google

Students will be expected to sign for this agreement electronically on school systems and a record kept of their acceptance to abide to this policy.

PARENT – ACCEPTABLE USE

School Policy

The world in which our students are educated is becoming increasingly dependent on the use of digital technology to provide next generation learning. At Culcheth High School, we embrace the educational opportunities that are presented by emerging technologies by allowing our students to collaborate, explore and investigate safely in a digital world.

This Acceptable Use Policy is intended to ensure:

- that our students will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use
- that the school network and users are protected from accidental or deliberate misuse that could put the security of the network and users at risk
- that parents/carers are aware of the importance of E-Safety and are involved in the education and guidance of young people with regard to their online behaviour

The school will endeavour to ensure that students will have the best possible access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work, if the school does NOT receive this form back Culcheth High School will assume you agree to this Acceptable Use Policy.

Permission Form

Name of Student:

Form:

- As the parent/carer of the above student I give permission for my son/daughter to have access to the Internet and to the school network including remote and cloud based systems
- I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, E-Safety education to help them understand the importance of safe use of digital technologies – both in and out of school
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and the school network
- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies
- I understand that my son's/daughter's activity on the school network will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy
- I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's E-Safety
- I allow my student to use the latest emerging technologies that Culcheth High School sees fit to enhance their educational experience

Parent/Carers Name:
Signed: Date:

STAFF – ACCEPTABLE USE

School Policy

The world in which our students are educated is becoming increasingly dependent on the use of digital technology to provide next generation learning. At Culcheth High School, we embrace the educational opportunities that are presented by emerging technologies by allowing our students to collaborate, explore and investigate safely in a digital world.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the Internet (including cloud based learning systems) and other communications technologies for educational use
- that the school network and users are protected from accidental or deliberate misuse that could put the security of the network and users at risk
- that staff are protected from potential risk in their use of digital technologies in their everyday work

The school will endeavour to ensure that staff will have good access to digital technologies to enhance their work, to enhance learning opportunities for students and will, in return, expect staff to agree to be responsible users.

Staff Acceptable Use Policy Agreement

I understand that I must use the school network and management systems in a responsible way, to ensure that there is no risk to my safety, to the safety and security of the school network and management systems and other users. I recognise the value of the use of digital technologies for enhancing learning and will ensure that students receive opportunities to gain from the use of these emerging technologies. I will, where possible, educate the young people in my care in the safe use of digital technologies and embed E-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school network and management systems, email, telephones and all other digital communications including cloud based systems
- I understand that the rules set out in this agreement also apply to use of the school laptop, cloud based and remote access systems out of school
- I understand that the school network and management systems are primarily intended for educational use
- I will not disclose my school network username or password to anyone else, nor will I try to use any other person's username and password
- I understand the "follow me" printing solution at Culcheth High School and will not let anyone else collect my printing work using my credentials
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the E-Safety Team
- I will be professional in my communications and actions when using the school network, e-mail and management systems
- I will ensure my email name and signature are setup correctly as per the school guidance
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school VLE) it will not be possible to identify by name, or other personal information, those who are featured
- I will not use chat and social networking sites on the school network
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner and should take place within clear and explicit professional boundaries
- I will ensure that all communications are transparent and open to scrutiny
- I must be aware that all my correspondents and communications are subject to the Freedom of Information Act 2000 and can be given to anyone who requests permission
- I will not engage in any online activity that may compromise my professional responsibilities
- I consent to the school monitoring and recording any use that I make of the school's electronic communications systems for the purpose of ensuring that the school's rules are being complied with and for legitimate business purposes. I will comply with any electronic communication policies that the school may issue

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not access personal e-mail addresses on the school network unless for educational purposes
- I will not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes, if an email contains an attachment and I do not know the person(s) I will reject it
- I will ensure that my data is regularly backed up, in accordance with relevant school procedures
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others and/or compromise the school network
- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will be mindful of large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings
- I will use removable storage devices (i.e. USB Memory Sticks) primarily for school use
- I will take every precaution to ensure that any removable storage device that I use is free from viruses

- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the local authority Personal Data Policy
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not keep files or information on Students/young people any longer than necessary

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- I understand that anything I produce for Culcheth High School during my working life is the copyright of Culcheth High School and should be treated as such.
- I understand that the work I produce for Culcheth High School should be kept on the school servers in either my Home Directory or Staff Resources and not on private devices to ensure this is accessible to others in my absence
- I understand that this E-Safety policy ensures that all School digital property remain accessible at all times

In relation to the use of a school laptop:

- I understand that I will be required to read and sign a Staff Laptop Loan Agreement

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of the school network and management systems in school, but also applies to my use of the school laptop out of school and my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action

School network definitions

For clarity listed below is what Culcheth High School class as “The School Network”

- Computer in ICT suites, normal classroom PC’s, Teaching Wall PC’s, iMac’s, Admin PC’s that include SIMS and/or FMS
- Mobile devices, iPads, iPods, Netbooks, tablets, Google Chromebooks, Macbooks, Apple TV’s, Spelling devices
- Wireless connections, inside of school and in the leisure areas such as the gym
- Google Apps for Education, Office 365, MyMaths, Maths Watch, Alfiesoft software, any school software which has be accessed in school or at home any software you login into from Culcheth High School

- Telephones and mobiles provided by the school for work use and educational visit use.

I have read and understand the above and agree to use the school network, ICT and management systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff will be expected to sign for this agreement electronically on school systems and a record kept of their acceptance to abide to this policy.

LAPTOP LOAN AGREEMENT

School Policy

Staff must be aware that their activities may be monitored and the work they produce in the course of their employment is the property and copyright of the school. In particular staff should note that the school network enables ICT staff to view individual computer screens remotely, to view records of internet sites visited and view emails (via the permission of the Headteacher). This may be necessary in the event of prolonged staff absence, or if there is reason to believe that communications are illegal or contrary to good professional practice. However, none of these will be undertaken in respect of school staff without the specific authorisation of the Headteacher.

It has been agreed that a laptop computer will be loaned to you while you remain employed at Culcheth High School. While the laptop is in your care, the following items should be noted:

- The laptop remains the property of Culcheth High School and is specifically for the use of the member of staff it is issued to. If loaned to another member of staff, the laptop remains the responsibility of the named member of staff
- Training in the use of the laptop and how to access the curriculum network, internet and email will be provided by Network Support Staff upon request. LEA and school policies regarding appropriate use, data protection, computer misuse and hand safety must be adhered to by all users of the laptop
- Should any faults occur, the school's Network Support Staff must be advised immediately so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware faults
- Anti-virus software is installed and must be updated. Network Support Staff will advise routines and will schedule this operation
- Only software licensed by the school, authorised by the School Network Manager and installed by Network Support Staff may be used. The use of unauthorised software is forbidden
- All data may be wiped off the laptop at any time for maintenance purposes and therefore data should not be stored on the hard drive of individual laptops: such information should normally be confined to a secure file server located in a secure place away from open access. Documents need to be stored in "My Documents" only
- The laptop may be called in for routine maintenance at any time by Network Support Staff and must be made available upon request
- I agree to the use the staff laptop in accordance with the Staff Acceptable Use Policy both in school and at home. I have read and signed the Staff Acceptable Use Policy
- In receipt of the laptop I agree to undertake further training on the use of ICT and the care and use of the laptop
- I agree to keep the laptop in good condition
- I agree to working with other teachers to develop the impact of ICT on teaching and learning in the school
- I agree that the laptop is for my use and I will not loan it to anyone other than another named teacher in the school
- I agree to ensure the security of the laptop at all times
- I will store the laptop in its correct case
- I agree to abide by the rules of the school's Data Protection Policy
- I agree that only software licensed by the school, authorised by the School Network Manager and installed by ICT staff may be used

- The laptop may be made available for routine maintenance on request by the Network Support Staff
- I agree to return the laptop to the school should I cease to be employed by Culcheth High School
- I agree that copying DVDs and CDs is a breach of copyright law. Under no circumstances can users copy or replicate a DVD or CD using the school's laptop. This includes all Compact Disc software packages, music CDs and DVD formats including movies
- The school will require your laptop to be returned if you are absent through long term illness or prior to taking maternity leave. The laptop should be returned before maternity leave to the Network Support Staff. In the event of long term sickness, the laptop will be returned to the school as soon as is possible by the owner

Staff will be expected to sign for this agreement electronically on school systems and a record kept of their acceptance to abide to this policy.

Laptop Make:

Laptop Model:

Serial Number:

Staff Name:

Received By (Signature):

Date:

DATA PROTECTION & DATA HANDLING GUIDELINES

Data Protection

Rationale

Culcheth High School is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the Data Protection Act 1998. The School needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to manage finances and to comply with legal obligations to funding bodies and government). To comply with the law, data about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Purposes

When processing data Culcheth High School will comply with the eight enforceable principles of good practice. They say that data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to countries without adequate protection

How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority [for use by schools only]
- the Department for Education (DfE)

- If you require more information about how we and/or DfE store and use your personal data, please visit:

- https://www.warrington.gov.uk/dataprotection

- If you want to see a copy of information about you that we hold, please contact:

- Amanda Crann – HR Manager Culcheth High School – aco@culchethhigh.org.uk
- Ian Mason – Information Governance Team - informationgovernance@warrington.gov.uk

Guidelines

1. The Data Controller for the school will be the Headteacher.

2. The school will register with the Data Protection Commissioner.

3. All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. Sensitive data will be kept in a lockable room with controlled access, or in a locked drawer or filing cabinet, or if computerised, password protected (N.B. See Technical and Cloud based systems)

4. Members of the school have the right to access personal data that are held by the school in electronic format and manual records. The LA has defined which information is viewable and a letter will be sent to parents and data subjects (see Student Acceptable Use Policy). Any individual who wishes to exercise this right should apply in writing to the Data Protection Controller. The school reserves the right to charge a fee for data subject access requests (currently £10).

5. The school must ensure that personal data are not disclosed to unauthorised third parties. The Act permits certain disclosures without consent so long as the information is requested; to safeguard national security; prevention or detection of crime including the apprehension or prosecution of offenders; assessment or collection of tax duty; discharge of regulatory functions (includes health, safety and welfare of persons at work); to prevent serious harm to a third party; to protect the vital interests of the individual, this refers to life and death situations.

6. The school will hold personal data for no longer than required. The school will follow the retention guidelines detailed in;

> "Records Management Society of Great Britain
> Local Government Group
> Retention Guidelines for Schools"
> Version 14/09/2004

7. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal of confidential waste, secure electronic deletion).

8. Data will be checked annually with data subjects.

Data Protection: Network Management and E-Safety

Personal data pertaining to staff, students and other individuals the School has dealings with is stored, in many cases, in an electronic format and held securely on the School Network. The nature of this storage, the security in place and the points of access are highlighted in this section of the policy.

An industry-standard educational management information system (Capita SIMS) is used to record and store data relating to students, parents of students, and staff. This system is accessible only to staff within the School, using a secure username and password, and can only be accessed via the School Network. Remote access is not granted to this system for Teaching staff only the Senior Leadership Team are able to access this outside of the school. The database is held securely on School Servers and stored locally.

A learning gateway application (My Ed App) provides a remote point of access, to parents who have a responsibility for a child, to their child's basic data. Currently, this gateway provides an overall attendance figure, a reason for absence and timetable information, and progress monitoring reports. Only parents with a responsibility for a child are provided with unique security access details to this system. They are required to agree, contractually, to an acceptable use policy each type they log in to the system.

Personal data pertaining to staff and students within the school may be extracted from the management information database (SIMS) for a variety of administrative and management purposes, and as such, may be held both on Staff Resources or Staff Userspace on the School Network. Both Staff Resources (a central data storage drive for Staff) and Staff Userspace (an individual data storage drive for a member of staff) are open to monitoring as indicated in the Culcheth High School E-Safety Policy, and Staff understand that the use of such personal data must be for professional purposes, and must be transparent and open to scrutiny.

A robust backup strategy protects all personal data held on the School Network from loss, and a robust firewall protects the data from unauthorised access both within and outside the School.

A remote-desktop service (CITRIX) allows staff to access both Staff Resources and their Staff Userspace from outside the School Network using a secure, online 'tunnel'. This service does not provide access to SIMS and Staff are not advised to use this service on a public computer.

Printing of personal data relating to both staff and students, for professional use, is limited in the main to office printers; however, a secure, 'follow-me' system of print management ensures that should such data be printed to one of the three curriculum printers, a secure access code is required by the member of staff.

A CCTV System is employed in parts of the School building, and on some occasions images are recorded for child protection and safeguarding reasons. In such instances, these recordings are held, only for a long as they are required, on a secure, office-based, stand-alone computer.

The School offers the rights for any child, or parent of a child, to request that they be excluded from school photographs. Photographs that are taken using school digital technology are held, only for as long as they are required, securely, and centrally within a shared Staff Resources Folder.

Finally, the Culcheth High School E-Safety Policy promotes a comprehensive Acceptable Use Policy for Staff in the use of the School Network and the Internet. Within the auspices of the

Acceptable Use Policy Staff agree specifically to "…only transport, hold, disclose or share personal information about myself or others, as outlined in the local authority Personal Data Policy".

Beyond this statement relating to the protection of personal data, the Culcheth High School Staff Acceptable Use Policy demands that Staff act professionally, openly, and transparently in relation to the use of digital technology, which includes the electronic use of personal data. Staff understand that they can be monitored and that they are open to scrutiny.

Data Handling

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office. for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles as listed above in the Data Protect Policy, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines "Personal Data" as data, which relate to a living individual who can be identified
(https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and
  Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Guidance for organisations processing personal data is available on the Information Commissioner's Office website:
https://ico.org.uk/for-organisations/guide-to-data-protection/

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data egg class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Secure Storage of and access to data

Culcheth High School will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them, particularly in the Staff Resources area. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords, which must be changed regularly. User passwords must never be shared. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods).

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- it is advised that the data is to be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups: snapshots taken at 07:00, 12:00, and full back up at 18:00 daily; cloud backup daily and tape backup weekly.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Google apps for education, Google docs and Google Classroom, this includes any other storage such as Dropbox, Microsoft 365 OneDrive or other cloud storage) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices, which contain personal data, must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Particular care should be taken if data is taken or transferred to another country, particularly outside
  Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Staff will be expected to sign for this agreement electronically on school systems and a record kept of their acceptance to abide to this policy.

EMAIL PROTOCOL GUIDANCE

Rationale

Electronic mail (e-mail) is seen as an invaluable method of communication for all staff at Culcheth High School; its greatest strength lies in the ability communicate to individuals and groups remotely. However, this very strength is also its greatest weakness; and an inappropriate use of this method of communication can in some cases lead to ambiguity and information overload.

It is crucial that e-mail is used appropriately and effectively. The aim of this protocol is to ensure that wherever possible this is achieved.

Protocol

In order to make the most effective use of Electronic Mail colleagues are asked to follow the protocol detailed below.

- E-mail messages should be brief and concise
- E-mail messages should never be flagged as urgent without prior consultation with the Headteacher
- E-mail messages should be sent only to those staff that need to receive the information; in short, colleagues should be efficient in their use of cc (carbon copy) e.g. Cc no response
- Any timescales quoted in e-mail messages should be appropriate and achievable
- Try to avoid attachments if possible
- Be aware at all times of safeguarding protocol when e-mailing student information
- E-mail messages should not be sent or read during teaching time
- I must be aware that all my correspondents and communications are subject to the Freedom of Information Act 2000 and can be given to anyone who requests permission
- My language and references within an email must be kept professional at all times ensuring the facts and reasoning for the content kept relative
- Emails produced by staff may appear in Student permanent files and used in more serious incidents involving the Police and/or authorities

Finally, even though we live in an increasingly digital age, dominated by electronic forms of communication, colleagues should be mindful of the fact that some information can and should only be communicated face to face. In short, there are many occasions where we have a professional duty to talk to colleagues rather than send an e-mail

SOCIAL MEDIA STAFF GUIDELINES

Definition of Social Media:

Websites and applications that enable users to create and share content or to participate in social networking.

As a result of the growing use of social networking sites (such as Facebook, Twitter, Instagram, Snapchat, Kik etc), we must be aware as a school of the implications of the use these social networking tools, and the potential impact activity may have on the school and the teaching profession. In general, the published guidance for safe use of social networking sites relates to young people and, whilst most of the content also holds true for adults, there are some additional points that should be considered by adults working with young people.

As a member of staff working in a school, you are entitled to a social life just like anyone else but it should be noted that, within your school community, you will always be linked to the school. This is complicated by the statement in the Teachers' Standards which states:

A. Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:

- *treating students with dignity, building relationships rooted in mutual respect, and at all times*

observing proper boundaries appropriate to a teacher's professional position teachers should;

'Uphold the law and maintain standards of behaviour both inside and outside school that are appropriate given their membership of an important and responsible profession'.

Staff should always remember that information published on their site may be read by their Headteacher, Governors, other staff members, parents or students. To prevent any misunderstanding, the following guidance is offered:

- Students and sixth form students are not online friends. It would be considered inappropriate to add students or sixth formers as friends on a personal site, the same could apply to parents. If you are looking to engage with the school community online, then consider using the school's official social media channels.
- Separate personal from professional. Decide from the start how you will use your account and the sort of information it will contain, if appropriate it may be necessary to create two separate accounts.
- Protect your information and make sure you understand the privacy settings and can restrict access to information you consider personal.
- Think about your profile picture. Most Social networking sites will display your profile picture even when your information is set to private. It will also show some of your friend's profile pictures. Consideration should be given to the content of any photographs chosen for inclusion on your personal profile.
- Think about what you are publishing. Although you may have set strict privacy controls, the information could still be shared by one of your 'friends'. It is sensible to assume that, once published, the
- information is no longer private. Inform your friend/relative you do not want a picture/video with you in it online.
- Be professional and do not discuss or disclose information relating to any aspect of your work, including the school, your colleagues, parents or students
- Watch who comments. Although you might be careful with what you are posting, it is possible that you may receive inappropriate comments, pictures or videos from your

contacts that will appear on your site. Remain vigilant of inappropriate items that are posted on your site that be viewed by others and ensure they are removed.

- Protect your digital image. Many sites now encourage you to name (tag) people that appear in uploaded photographs. These tags can be indexed and the original photographs displayed in search results. Even though you don't post pictures you may find that your friends do.
- Talk to your friends and contacts. If it is a personal site, friends and contacts should understand the need to keep your information private and ensure inappropriate or potentially embarrassing comments, pictures or video are not posted on your site. If it is a professional site, they need to understand why you may not add them as friends or, if they are, the types of posts or comments that are acceptable.

If in doubt, ask

What is my on-line reputation?

Your online reputation is the perception, estimation and opinion that is formed when you are encountered online. This could be when someone visits your social networking profile, but could also be when anyone reads a comment you posted on another profile. It could also be when someone sees your online photo albums or an image with you in it, indeed any instance or reference of you that either you posted or someone else did. It is what your digital footprint says about you.

Your online reputation will be formed through:

- Postings by you
- Postings by others but about you or linked to you
- Postings by others pretending to be you

How is your online reputation different?

Remember that the Internet never forgets - when you post something online it will always be there.

Deleting is almost impossible from Social Media websites if your content gets into the wrong hands, it could be copied indefinitely. Social Media sites have no obligation to remove anything it is classed as “Free Speech”.

What can affect my on-line reputation?

	Comments	Photos	Films	Groups/Affiliations
Postings by you	• Inappropriate comments about other people or staff at your school. • Comments that you have made about other people's reputation. • Defamatory comments you have posted about others photos or films • Inappropriate language and poor grammar • Publishing misleading or fraudulent information about you or others	• Nights out on the town. • Prank photographs of others that have been posted without their permission. • Photos that compromise the security of others that could be interpreted as bullying.	• My two weeks in Ibiza or Aya Nappa. • Films put up of members of staff without their permission. • Re distributing content on YouTube • Posting content without copyright or license to do so	• School rugby team and other robust groups where the pressure is on to be defamatory. • Gaming clans or guilds where there is online taunting and posturing • Inappropriate friends or group, e.g. radicalisation and racial hatred etc.
Postings by others but linked to you	• Comments posted by children or their parents, commenting on your work or professionalism. • Retweets of things you said in confidence. • "friends" posting comments with inappropriate language on your profile	• Tagging you in a photo from a staff night out		• Suggesting you are a member of an inappropriate group
Postings by others pretending to be you	• Someone logging into your social networking account and changing or posting information apparently on your behalf (known as FRAPE) • Comments posted apparently by you but expressing extreme of defamatory views	• Mistaken identity - distributing pseudo pornographic images - images made to look like you	• Third party posting inappropriate films on YouTube but spoofing your identity as if they were posted by you.	• Suggestions that you are a member of an extremist group for example.

Managing your Privacy settings-using privacy effectively

- Test your privacy- find out from your friends what information they can see on your profile. Use http://www.reclaimprivacy.org/ to scan your profile privacy settings
- Discuss expectations with friends. Are you happy to be tagged in a photo?
- Familiarise yourself with our policies and procedures
- Limit your online information in Google searches
- Remove yourself from Facebook searches
- Manage your friends lists and redefine access you allow to your content – Do you know each and every one of your friends/followers?
- Manage your online photos and albums
- Explore what other applications access your online profiles
- Does your physical location (Geotagging) appear online?
- Look for photos you are 'tagged' in
- Regularly review your privacy settings and amend accordingly

When posting online consider

- Scale - global platforms – Millions of users
- Permanency - once it is online it is there forever – You have no control once your content is uploaded, anyone with access could copy this

- Audience - public or private? Friends, friends of friends or everyone?
- Use the technology to its full potential but just be aware of the pitfalls and think before you post.

Further reading

- Facebook Safety pages - http://www.facebook.com/safety
- Facebook Safety pages for educators - http://www.facebook.com/safety/groups/teachers/
- Cyberbullying Advice produced by Childnet and commissioned by DCSF in 2007 that builds on the 'Safe to Learn' guidance - http://www.digizen.org/resources/cyberbullying/overview/

Resources

- Let's Fight it Together - http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx

Support and Advice

- POSH - Professionals Online Safety Helpline - www.saferinternet.org.uk/helpline.Provided by the
- UK Safer Internet Centre, a helpline dedicated to supporting professionals who work with children in the UK with Online Safety related issues
- helpline@saferinternet.org.uk or 0844 3814772

As a member of staff at Culcheth High School I will follow these guidelines to the best of my ability. If I am unsure I must ask for help with the appropriate person responsible within the school.

E-Safety Reference & Links

Legislation

Culcheth High School has produced this E-Safety Policy and guidance with the help of the acts below. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an E-Safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;

Prevent or detect crime or in the interests of national security;

- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material, which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear,
on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1999

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo- photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material, which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of

“higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching- and-confiscation

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website: http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Links

Culcheth High School – E-Safety

Safer Internet Centre

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

Cyberbullying - http://cyberbullying.org/

Guidance:

Social Media Guidance for Parents

Facebook Guide for Parents

Social Media Guidance for Teachers

Safer working practises for adults who work with Children

Training / Awareness of this policy

Members of staff will be made aware of the school's password policy:

- at induction
- Staff Handbook
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

Parents/Community

- On the school's website
- Newsletters

Audit / Monitoring / Reporting / Review

The responsible person will ensure this policy is up to date:

- E-Safety Manager, yearly review
- Governing Body – Significant changes present to them
- E-Safety Team, regular updates review