THE SHROPSHIRE GATEWAY EDUCATIONAL TRUST

E-SAFETY POLICY

Consulation	Local Governing Bodies
Review Cycle	Annual
Date Approved	Nov 2016
Approved By	SGET Board
Next Review Date	Nov 2017

Contents

Introduction

The Shropshire Gateway Educational Trust believes that the safe use of information and communication technologies in schools and education settings brings great benefits. Recognising online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This Policy template will help schools and settings to form an online safety (or 'e-Safety') policy that is appropriate to their needs and requirements.

The trust:

- believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience
- has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

Purpose of Policy

The purpose of this policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that each trust school is a safe and secure environment.
- Safeguard and protect all members of the each school's community online.
- Raise awareness with all trust schools regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including trustees, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- This policy must be read in conjunction with other relevant trust policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, Acceptable Use Policies, confidentiality.

E-Safety Committee

The school safety committee is convened by the e-safety officer. It will meet once per term and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, parents, pupils.

Internet use and Acceptable Use Policies (AUP's)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role (Appendix i)

A copy of the pupil Acceptable Use Policies will be sent to parents with a covering letter/reply slip (Appendix ii)

Acceptable Use Policies will be reviewed annually.

These Acceptable Use Policies will form part of the first lesson of ICT for each year group.

The Prevent duty

The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

All staff should be aware of the following

1. DfE Prevent duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel

The Prevent duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be use (Appendix iv)

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection act.

The unauthorised Photography of pupils by of other pupils in school should not be permitted.

Mobile phones and other devices

Pupils' mobile phones should be handed into the office at the beginning of the day and collected by the pupil at the end of the day.

STAFF/Visitor Mobile Phones in Primary Schools

To ensure the safety and welfare of children all primary schools operate a policy which stipulates that personal mobile phones, cameras and video recorders cannot be used when in the presence of children, on the premises or when on outings.

Schools will ensure that:

- All mobile phones will be kept in the staffroom/office throughout contact time with children (this includes all staff, visitors, parent helpers, supply teachers and students)
- Parents are not allowed to use their mobile on the school premises. If you find a parent doing this you should inform them of this and refer them to the Headteacher
- Mobile phones will not be used in any classroom. In the event of a personal emergency the school phone may be used. Alternatively a personal call can be made from an individual's mobile in the staff room.
- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. Only school property can be used for this.
- Photographs and recordings can only be transferred to, and stored on a school computer.
- During school outings staff will have access to the school mobile or may choose to use their own for emergency communication only. If staff use their own phones for emergency communication they are advised to make another member of staff aware.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Use of e-mails

Pupils should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'). All users should be aware that the ICT system is filtered and monitored.

Staff should ensure that sensitive data such as email or Student Information Management Software in a classroom on a computer is not displayed on an overhead projector.

Data storage

Only encrypted USB pens are to be used in school.

Reporting

All breaches of the e-safety policy need to be recorded in the school's ICT reporting book. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require SLT intervention (eg cyberbullying) should be reported to SLT in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg Ceop button, trusted adult, Childline)

Social networking and Personal Publishing

The school will control access to social media and social networking sites using internet filtering software. Access is currently denied except for collaboration tools within the Office 365 portal hosted by the school.

Pupils are advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and email addresses, full names of friends/family, specific interests and clubs etc.

Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Inspect any background detail in a photograph which could identify the student or his/her location.

Staff official blogs or wikis should be password protected and run from Office 365 portal with approval from the Senior Leadership Team. Staff are advised not to run social network spaces for pupil use on a personal basis.

If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.

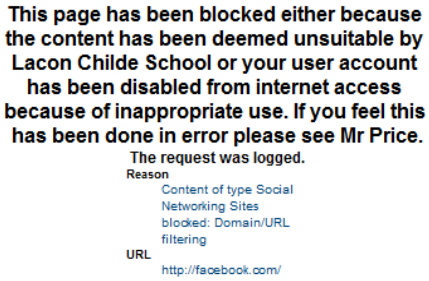
Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Internet Filtering

The school will work with Novus as ICT support provider and Smoothwall to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported through line management and the ICT support desk.

Schools' broadband access will include filtering appropriate to the age and maturity of pupils. If a website is filtered and access is denied, users will receive a message similar to the example below. If the security software has denied access unnecessarily a message should be sent to the ICT support desk. Access will then be granted for relevant users.



Education of Pupils

To equip pupils as confident and safe users of ICT each school will undertake to provide:

- A planned, broad and progressive e-safety education programme that is fully embedded for all children , in all aspects of the curriculum, in all years.
- Regularly auditing, review and revision of the ICT curriculum
- E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
- Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc

Additionally:

- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour
- Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

- A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
- E-safety training is an integral part of Child Protection / Safeguarding training and vice versa.
- An audit of e-safety training needs is carried out in line with the needs of each school and is addressed.
- All staff must have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures carried out on an annual basis
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy.
- Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate.
- The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety.
- The school takes every opportunity to research and understand good practice that is taking place in other schools.
- Governors are offered the opportunity to undertake training.

Monitoring the use of the Learning Platform

All staff will monitor the usage of the Learning Platform by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

Pupils/staff must apply the rules outlined in the 'Responsible Computer & Internet Use' posters

Only members of the current pupil, parent/carers, governors and staff community will have access to the Learning Platform.

All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.

When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP for the user may be suspended.

- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.

A visitor may be invited onto the collaborative documents platform by a member of the school community. Pupils require approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Parents and the wider community

There is a planned programme of e-safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety co-ordinator with input from the e-safety committee.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the Trust's policy on anti-bullying.

All incidents of cyberbullying reported to the school will be recorded.

- There are clear procedures in place to investigate incidents or allegations of Cyberbullying. These are managed by the Pastoral Team.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

Monitoring and reporting

The school network provides a level of filtering and monitoring that supports safeguarding.

The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

The records are reviewed / audited and reported to:

- the school's senior leaders

- Governors
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

The school action plan indicates any planned action based on the above.

Appendix 1 – Acceptable Use for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

Signed _____

Appendix 1 cont. - Acceptable Use for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed _____

Appendix 1 cont. - Acceptable Use for learners in KS3 and above.

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- set strong passwords which I will not share
- not use my own mobile device in school unless I am given permission
- respect copyright and the intellectual property rights of others
- only create and share content that is legal
- always follow the terms and conditions when using a site
- only visit sites which are appropriate
- discuss and agree my use of a social networking site with a responsible adult before joining
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I am aware of the CEOP report button and know when to use it.

continued…

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- forward chain letters
- breach copyright law
- do anything which exposes others to danger

I accept that my use of the schools ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

Appendix 1 cont. - Acceptable Use for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the Trust's ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

Appendix 1 cont. Acceptable Use for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

<School Name>

Parent / guardian name:……..

Pupil name: ……

Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent's signature:…… **Date:**…….

Appendix 3 – Photo/video consent

School Name:

Name of child:

Class:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.

To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please bring the completed form to the ceremony. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

1. May we use your child's image in our printed promotional publications? Yes / No

2. May we use your child's image on the school website? Yes / No

3. May we record your child's image on our promotional videos? Yes / No

4. May we use your child's image in the local press? Yes / No

5. May we use your child's image in the school's social media accounts? Yes/No

Signature: Date:

Your name (in block capitals):

Appendix 4 – Links

Shropshire Council Education Improvement Service documentation

https://www.shropshirelg.net/supporting-teaching-and-learning/e-safety/

The Safe Use of New Technologies - *The Safe Use of New Technologies report is summary of findings from OFSTED based on 35 e-safety inspections carried out in a range of settings:* http://bit.ly/9qBjQO

BBC WebWise: http://www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

Appendix 5 – Clee Hill Community Academy

Mobile Phones

At Clee Hill Community Academy, mobile phones will be kept in the office and staffroom at all times. However, on school trips, personal mobiles may be used in emergency situations to contact the school.

In line with our online assessment, the use of photographs and recordings may be accessed outside of school if it is for the purpose of online assessment (Tapestry or equivalent). These photos are shared online with parents as part of the assessment process.

Photographs may be stored online for media purposes (i.e. producing posters or displays for the school) which is in line with parental photo consent forms.

Preventing extremism

A record is kept of all staff and governors who have attended PREVENT training. Information and advice for parents and staff can be found on the Stay Safe noticeboard.

Appendix 6 – Cleobury Mortimer Primary School

The Leadership team member responsible for e-safety is:

The governor responsible for e-Safety is:

The designated member of staff for child protection is:

The e-Safety Coordinator is:

The policy is available for parents/carers at:

Date of E-safety training for staff

Date of Prevent training

Appendix 7 – Lacon Childe School

The Leadership team member responsible for e-safety is:

The governor responsible for e-Safety is:

The designated member of staff for child protection is:

The e-Safety Coordinator is:

The policy is available for parents/carers at:

Date of E-safety training for staff

Date of Prevent training

Videoconferencing

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.

Users

Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing should be supervised appropriately for the pupils' age. Parents and carers should agree for their children to take part in videoconferences. This will be in the annual return.

- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

- Content
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

Mobile phones & devices

Lacon Childe School accepts that parents equip pupils with mobile phones and other mobile technologies for educational, social and safety reasons. The widespread use of mobile phones by young people requires that all staff, students, and parents take steps to ensure they are used safely and responsibly at school. This policy is designed to ensure that potential issues involving mobile phones and electronic devices can be clearly identified and addressed, ensuring the benefits they provide (such as increased safety) can continue to be enjoyed by our students.

Responsibility

It is the responsibility of pupils to follow the guidelines in this document if such a device is taken to school. Parents should also be aware of, understand and support the guidelines if their child brings a mobile phone or device into school.

Acceptable use

Mobile phones and other mobile technologies belonging to students may be handed into the school office before the start of the school day and collected at the end of the day. If not handed in all mobile phones and electronic devices must be switched off and kept out of sight during the school day, including break and lunchtime, and at any time on the school grounds. There may be exceptions to this rule if a teacher has requested that such equipment is necessary for a particular lesson and pupils are directly instructed to make use of the device. The device will be the responsibility pupil and school will not be responsible for damage, loss or theft. Staff will be issued with a school phone where contact with pupils is required. Passwords or pin numbers are essential for any device used on school property to comply with data protection guidelines. Parents must always contact the school office as the first point of contact and never a pupil directly as this will ensure your child is reached quickly and assisted in the appropriate way.

Unacceptable use

Mobile phones or other personal mobile communication technologies will not be used in school unless permission is granted by a member of staff. This applies to any function of such technologies such as, photography, email, internet search, video, calculator or any other application. Mobile technology must not be taken into any exam situation, and contravention of this clause can lead to disqualification from an exam series by all examination boards. It is forbidden to record any member of the school community on personal devices or to upload images of the school to websites for public viewing without permission from the Head Teacher, and any pupil who contravenes, or supports others in this behaviour will be liable to serious disciplinary action. Electronic devices must not be used to bully, embarrass or cause discomfort to any other pupil, member of staff or visitor to the school. The sending of abusive or inappropriate text, picture or video messages is forbidden.

Confiscation of mobile phones

Pupils who break the rules set out in this document will have their devices confiscated by staff. The mobile device will be taken to the school office and kept until the end of the school week unless collected by a parent or guardian. The school office will keep a record of any mobile device confiscated as well as any subsequent collection by parents/guardians. If the device is confiscated again then it will be kept until it can be collected after a meeting between parents and a senior member of staff.

School Owned Mobile Devices

The school provides a variety of mobile devices for teaching and learning activities. These are to be used in accordance with the displayed Acceptable Use Guidelines and are bookable by staff using the https://laconchilde.roombookingsystem.co.uk/ system. Mobile devices should be returned immediately to the Network Manager following a booked session to allow essential maintenance and charging to be carried out.

Devices should be returned in the same condition. This includes the removal of any data, photos or videos recorded during the loan period. Any data on such devices should be uploaded to Cloud services immediately and not be stored on individual devices.

Appendix 8 – Stottesdon C of E School

The Leadership team member responsible for e-safety is:	**Katie Jones**
The governor responsible for e-Safety is:	**Sarah Price**
The designated member of staff for child protection is:	**Katie Jones/Tracy King**
The e-Safety Coordinator is:	**Katie Jones**
The policy is available for parents/carers at:	**www.stottesdon.shropshire.sch.uk**
Date of E-safety training for staff	**PD Day September 2016**
Date of Prevent training **February 2016**	**25/11/15 and Tracy King Training**

Infringements and sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / contact with parent]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

- Ensure appropriate technical support filters the site
- Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

- Secure and preserve any evidence
- Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

The school is likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Appendix 9 - Implementation Plan

Is training required to implement this policy?	**Yes** ☐ **No** ☐
If Yes, how will this be delivered and by whom?	
To which groups of staff does this policy need to be issued?	*All school staff and Trustees.*
How will the policy be issued and by whom?	*Via email from Head teachers* *Via Chairs of LGB*
Date adopted by Local Governing Body:	
Signed (Chair of LGB)	
Name of School	

Appendix 10 - Equality impact assessment screening form

Section one: screening for impact	
Name of policy	
Project lead completing assessment:	Matt Hayes
Position:	Business Manager

1. What is the main purpose of the strategy/project/policy?

Provides staff with a framework for grievances in a way that promotes fairness, transparency and equality.

2. Who will be the main stakeholders/users of the policy? Please consider the impact of the policy on the different groups of stakeholder /users.

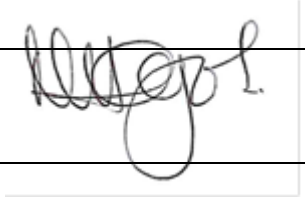
Headteachers, Staff and Trustees.

3. Use the table to show:

- Where you think that the policy could have a negative impact on any of the equality strands, that is, it could disadvantage them – if no impact please note the evidence for this.
- Where you think that the strategy/project/policy could have a positive impact on any of the groups or contribute to promoting equality, equal opportunities or improving relationships within equality characteristics.

	Positive impact	Negative impact	No impact	Reason and evidence (provide details of specific groups affected even for no impact)
Age				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.
Disability				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.
Gender				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.
Gender identity				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.

Sexual orientation				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.
Race				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.
Religion or belief				The policy provides all staff groups with an opportunity to raise any concerns they may have regarding equality and diversity.

4. If you have indicated there is a negative impact on any group, is that impact:		
Legal? (not discriminatory under anti-discriminatory legislation)	Yes ☐	No ☐
Intended?	Yes ☐	No ☐
Level of impact?	High ☐	Low ☐
If the negative impact is possibly discriminatory and not intended and/or of high impact you must complete a full equality impact assessment. If not, complete the rest of section one below.		
5. Could you minimise or remove any negative impact that is of low significance? Could you add any additional action to have a positive impact rather than no impact?		
N/A		
6. If there is no evidence that the strategy, project or policy promotes equality, equal opportunities or improved relations – could it be adapted so that it does? If so, explain how.		
N/A		
7. Please list the outcome following this equality impact assessment (this could be no changes, some changes, further work needed around particular groups or cease development of the policy).		
N/A		
Signed: 		Date: