THE CORBET SCHOOL

E-Safety & Acceptable Use Policy

Associated Policies

- Child Protection Policy
- Extremism and Radicalisation Policy
- Anti-Bullying Policy
- Home school agreement
- Prevent Duty
- Channel Programme
- Keeping Children Safe in Education

Policy Manager:- A. Millward

Review Completed:- September 2019 **Review Period:- Annual**

Next Review Due:- September 2020 **Approval Authority:- SLT**

Contents Page

Responsibilities

The Head teacher has overall responsibility

The member of SLT team with operational responsibility for e-safety is Alison Millward who is also the designated safeguarding lead

The governors appoint a Link Governor to support e-safety.

The Lead Teacher for ICT is Daniel Goodall

The Network Manager is Keith Rendall

Any e-safety concerns will be co-ordinated by the Corbet School Pastoral Team in the first instance.

The Senior member of staff is responsible for attending the safer schools meeting and discussing e-safety matters with all attending stakeholders, delivering staff development and training, co-ordinating the recording and reporting of incidents along with any developments and liaising with the local authority and external agencies to promote e-safety within the school community. She may also be required to deliver sessions for parents.

Safer Schools committee (including e-safety)

The safer schools' initiative committee is convened by Julia Kear (Assistant Business Manager). It will meet once per annum and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, parents, pupils, police and representative from Shropshire LA

Internet use and Acceptable Use Policies (AUP's)

All members of the school community will sign an Acceptable Use Policy that is appropriate to their age and role. Examples of the AUPS used can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip. This can be found in appendix 2. School will install a on line reminder of the AUP that will provide regular reminders to pupils and will ask them to confirm they have read the policy.

AUP's will be reviewed annually. All AUP's will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

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 used.

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 GDPR. (data protection regulations)

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.

Mobile phones and other devices

All mobile phones (pupils and staff) should be switched to silent or off whilst on the school premises. Pupil phones found to contravene this should be confiscated and taken to the school office. Confiscated phones can be collected at the end of the school day from reception (see rules/sanctions displayed in classrooms for further guidance).

There may be times when some of the features of mobile phones may be beneficial to the learning activities in a lesson (eg pupils may wish to capture photos/videos of an experiment). In such cases mobile devices can be used once permission has been granted by the teacher.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails

Pupils and staff 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 and staff 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. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. 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.

Data storage

Only encrypted USB pens are to used in school. Staff need to risk assess any data that they plan to temporarily store on a USB pen to ensure that any potential loss has minimal impact.

Reporting

All breaches of the e-safety policy need to be recorded using the normal online reporting systems or via written reporting if it is a child protection issue. 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 regarding radicalisation/extremism (The Prevent Duty) should be referred to the designated safeguarding lead immediately.

Incidents which are not child protection issues but may require further intervention (eg cyberbullying) should be reported to the pastoral team 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'. In the event of an allegation against the Headteacher, the teacher in charge of Child protection should be notified (Alison Millward). 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)

Infringements and sanctions

Whenever a student or staff member 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:

(a) Students

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

Pupil to be placed in detention (removal of phone). Detention to be logged in pupil's planner and on Sims

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

Pupil to be placed in after-school detention (removal of phone). Detention to be logged in pupil's planer, a detailed reason provided for parental letter and logged on Sims

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

Inform SLT immediately and record information on Sims. SLT to investigate further and issue appropriate sanctions e.g. whole school detention, Internal exclusion or Fixed term exclusion. Parents to be informed immediately.

Other safeguarding actions

If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site
2. 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

Inform SLT immediately and record information on Sims. SLT to investigate further and issue appropriate sanctions e.g. Fixed term exclusion, Permanent exclusion. Parents to be informed immediately. School to contact Police and LA e-safety officer if required.

Other safeguarding actions:
1. Secure and preserve any evidence
2. 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.

(b)Staff (All working members of the school)

Level 1 infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - Headteacher. Warning given.]

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- 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.

[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police.

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
2. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are 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.

Social networking

Pupils

Pupils are not permitted to use social networking sites within school.

Staff

It is recognised that social networking sites have a major role to play in today's society. However, staff must be aware of the following:

Staff must not add pupils as friends in social networking sites**.
Staff must not post pictures of school events without the Headteacher's consent
Staff must not use social networking sites within lesson times
Staff need to use social networking in a way that does not conflict with the TDA Core Standards or Personnel handbook or Shropshire Local Authority Professional Code of Conduct for Staff Working in Schools.
Staff should review and adjust their privacy settings to give them the appropriate level of privacy.

Note** - There may be occasional exceptions to this rule. Eg where a staff member has a close relative at the school who is a pupil, such as Mother & Daughter.

Staff communication

Staff should only communicate with pupils and parents through official channels. These channels include:

- Post on school letter headed paper
- School telephone system
- School provided mobile phone
- School e-mail system
- School provided video conferencing solutions

The following are excluded from the official channels:

- Social networking sites
- Gaming sites
- Chatrooms
- Personal mobile phones
- Personal e-mail addresses
- Personal video conferencing solutions (eg Skype)

Such contact could lead to disciplinary action.

Education

Pupils

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

a). 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.
b). Regular auditing, review and revision of the ICT curriculum
c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc

Additionally,

a). 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
b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
c). The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour
d). 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 - this may be done via level 1 CP training.
- E-safety incidents and concerns are addressed with all members of staff as and when required.
- E-safety incidents are a standing item at Senior Leaders weekly meetings.

Parents and the wider community

There are 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.

Monitoring and reporting

a). The impact of the e-safety policy and practice is monitored through the safer schools committee meeting and events on incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

b). The records are reviewed and reported to:

- the school's senior leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

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

d). The Corbet School keep a database of out of school interaction between staff and pupils e.g. clubs/activities that pupils and staff may attend, staff and relationships to pupils e.g Aunts/Uncles etc.

Appendices

Appendix 1 – AUP’s

AUP Guidance notes for learners

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 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 immediately

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 school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

Acceptable Use Policy (AUP) Guidelines for any adult working with learners

- ***This 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 school 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 (e.g. Facebook, Twitter, Instagram, 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 IT misuse to the named e-Safety officer.
- Promote any supplied E-Safety guidance appropriately.
- Return school IT equipment to the school without delay at the request of the IT Department or School Senior Leadership Team.

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 overleaf…

I agree that I will not:

- Visit internet sites and make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to;
    - Pornography (including child pornography).
    - 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.
- Enter into any communication that may bring The Corbet School, or its staff, pupils or any other stakeholder into disrepute.
- Do anything which exposes others to danger.
- Access 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 school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Staff Full Name:	
Staff Signature:	
Date:	

AUP Guidance notes 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 acknowledge that my child will have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school as part of their learning. 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 – Links

(a) Shropshire Council Advisory Service documentation

All Advisory Service e-safety documentation can be found at:

https://www.shropshirelg.net/esafety/staff/Pages/welcome.aspx

(b) 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

(**c) 360 degree Safe**

The policy guidance is based upon criteria with the 360 degree safe framework. The framework can be found at:

http://www.360degreesafe.org.uk

(d) **Shropshire Safeguarding Contact details:**

Local Authority Designated Officer (LADO)	lado@shropshire.gov.uk
Emergency Duty Team	0345 678 9040
01743 249544 (Out of hours only)	