E-Safety Policy 2020

This e-safety policy has been developed by the E-Safety Working Party at Chad Vale Primary School following the 360 Safe audit of provision for e-safety.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Board of Directors / Governing Body / Governors Sub Committee on:*	*October 2019*
The implementation of this e-safety policy will be monitored by the:	*Kerry Grosvenor / Paul Samson*
Monitoring will take place at regular intervals:	*Ongoing and reported to governors via the termly Headteacher's Report*
The *Governing Body* 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:	*Within Headteacher's termly report to govenors*
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:	*November 2018*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Andy Pyper (Link2ICT)*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *students / pupils*
  - parents / carers
  - *staff*

CHAD VALE RESPECTING RIGHTS

This policy is written with consideration to our schools commitment to the Rights of the Child (UNRC) and our achievement of becoming a Rights Respecting School. Although direct reference to this is not continuously made, the policy has been written with full awareness of our responsibility and commitment to this purpose.

As a school we have decided that the following rights link to this policy:

Article 3: Everyone who works with children should always do what is best for each child.
Article 16: We have the right to privacy.
Article 19: You have the right to be looked after and kept safe from harm.
Article 36: We have the right to be protected from doing things that could harm us

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

The Education and Inspections Act 2006 empowers the Headteacher 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. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to 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 (see appendix for template policy). 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

Governors:
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 Safeguarding *Governor which will* include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

- **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 Co-ordinator.
- **The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management 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 / Principal / Senior Leaders are responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Principal / 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.
- The Senior Leadership Team will receive regular monitoring updates from the E-Safety Co-ordinator Officer.

E-Safety Coordinator:

- leads the e-safety committee.
- takes day to day responsibility for e-safety issues and has a leading 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.
- provides training and advice for staff.
- liaises with the Local Authority / relevant body.
- liaises with school technical staff.
- receives reports of e-safety incidents and monitors SIMS log of incidents to inform future e-safety developments.
- meets with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs.
- reports regularly to Senior Leadership Team.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Headteacher/Deputy Headteacher for investigation/action/sanction.
- all digital communications with students/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 / pupils understand and follow the e-safety and acceptable use policies.
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Senior Person for Child Protection

Will 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.

E-Safety Group

Members of the E-safety Group will assist the E-Safety Co-ordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- monitoring network / internet / incident logs.
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision.

- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (KS1 AUP / KS2 AUP).

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, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school / academy* 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, social media pages and on-line pupil records (SPTO)
- their children's personal devices in the school / academy (where this is allowed).

Community Users:

Community Users who access school systems will be expected to sign the AUP before being provided with access to school systems.

Policy Statements:

Education – students / pupils

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 is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned e-safety curriculum is provided, followed and regularly revisited throughout the curriculum.**
- **Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.**

Education – parents / carers

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

- Curriculum activities.
- Letters, newsletters, web-site, social media, Marvellous me.
- Parents evenings/sessions.
- High profile events / campaigns eg: Safer Internet Day.
- Reference to the relevant web sites / publications.

Education & Training – Staff/Governors/Volunteers

- 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.
- 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.

- This E-Safety policy and its updates will be presented to and discussed by staff in INSET days and briefing meetings.
- The E-Safety Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

- There will be ongoing monitoring of the safety and security of school systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password, (using letters, numbers and symbols.) Users are responsible for the security of their username and password although class teachers will also hold a list their pupils log-on details, this is should kept in a safe place.
- The network and email administrator passwords for the school must also be available to the Headteacher and kept in the school safe.
- The ICT Co-ordinator 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 via Link2ICT.
- Computer use in school is monitored continually using Policy Central Enterprise software.
- Technical support is managed by CloudW.

Bring Your Own Device (BYOD)

- The school has a set of clear expectations and responsibilities outlined in the BYOD User Agreement, which must be signed by pupil and parents before devices are used in school.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Pupils receive training and guidance on the use of personal devices.
- Monitoring of usage will take place to ensure compliance.

Use of digital and video images

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images must not be published or made publicly available on social networking sites and must also follow the new GDPR regulations.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication

of those images, also in line with GDPR regulations. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Staff / Pupils and Parents must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images. Photos will ONLY be published if permission has been given on GDPR forms.
- Pupils names will not be used anywhere on a website or blog, in association with photographs.
- Written permission from parents or carers will be obtained before photographs and work of pupils are published on the school – GDPR.
- Where requests are made for 3rd party use of images (e.g. newspaper reports/external websites) additional signed photo consent is required from parents/carers.

Data Protection
The school / academy must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy.**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).**

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

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

- the data must be encrypted and password protected.
- the device must be password protected.
- the device must offer approved virus and malware checking software.
- 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.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students /

pupils should therefore use only the school email service to communicate with parents, pupils, teachers and external agencies.

- Users must immediately report, to the nominated person – in accordance with the school / academy policy, 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 students / pupils or parents / carers (email, Schoolcomms, social media, MarvellousMe) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website or social media feeds and only official school email addresses should be used to identify members of staff. These are available on our school website too.

Social Media - Protecting Professional Identity

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff members must ensure that they set the privacy levels of their social media to 'strict/high/friends only' so that pupils and parents cannot view personal photos, updates or comments

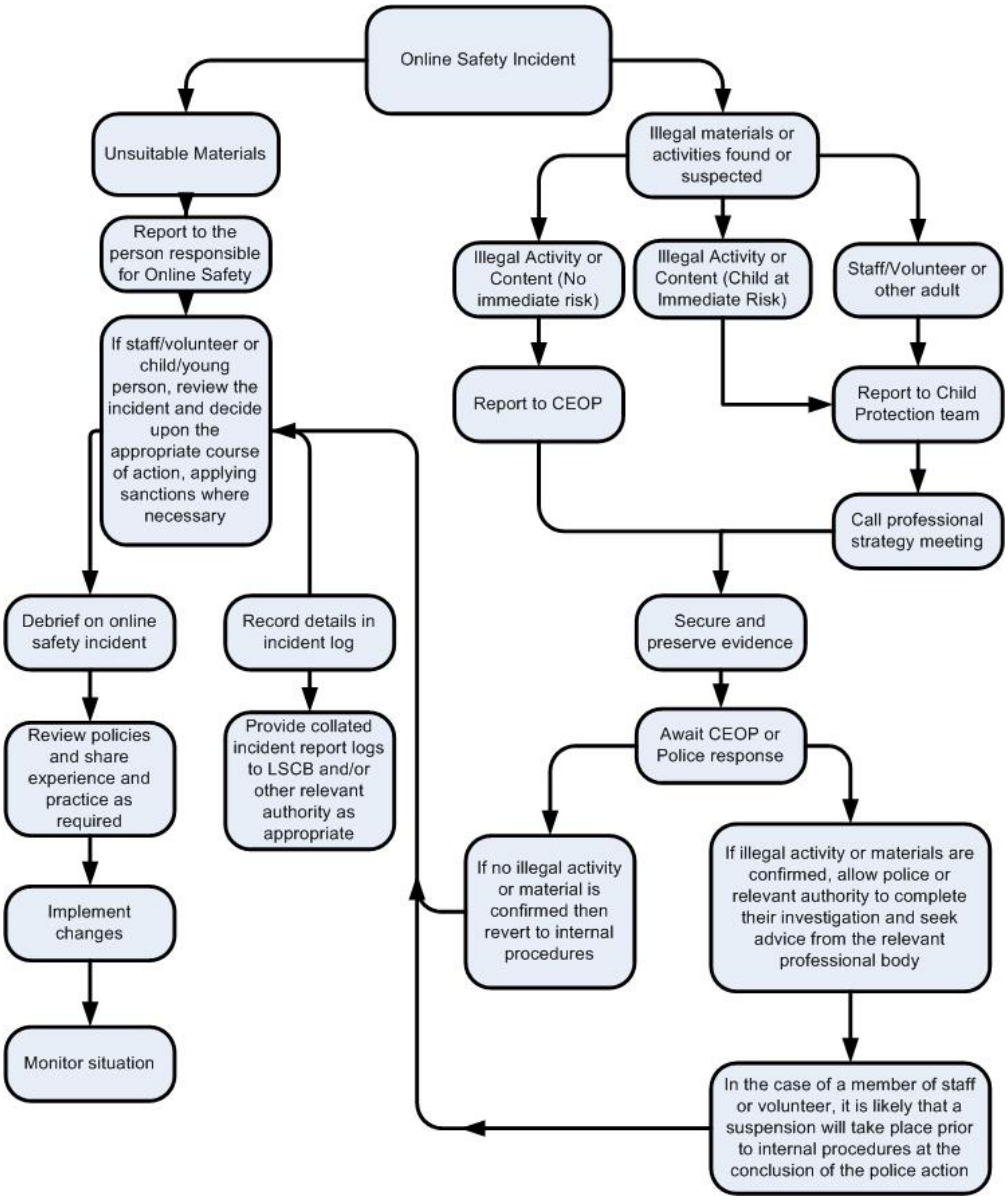
The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the school policies. See also Social Media Policy.

Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents:

It is hoped that all members 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 in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer 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 for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet 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. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- 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.
    - other criminal conduct, activity or materials.
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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 form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions:

It is more likely that the school / academy 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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to ICTCo-ordinator	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning/Behaviour Record	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X		X
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	
Unauthorised use of social media /messaging apps / personal email		X						X	
Unauthorised downloading or uploading of files		X							
Allowing others to access school / academy network by sharing username and passwords		X							
Attempting to access or accessing the school / academy network, using another student's / pupil's account		X							
Attempting to access or accessing the school / academy network, using the account of a member of staff			X						
Corrupting or destroying the data of other users			X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	?		X		X	
Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X		X	
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident			X			X		X	
Deliberately accessing or trying to access offensive or pornographic material			X	?		X	X		X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			**X**	**?**	**X**	**X**	**X**	**X**	**X**

Staff **Actions / Sanctions**

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X				X
Inappropriate personal use of the internet / social media / personal email		X				X		
Unauthorised downloading or uploading of files		X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X						X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		?				X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		X						X
Actions which could compromise the staff member's professional standing		X	?			X		
Actions which could bring the school / academy into disrepute or breach		X	X			X		

the integrity of the ethos of the school / academy								
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X					X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X						X