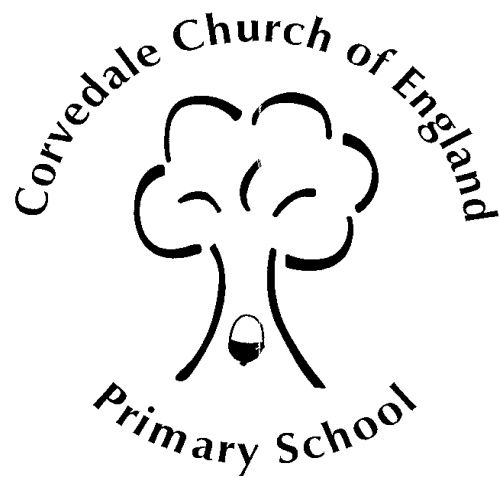


**Corvedale C of E Primary School**  
**E-safety policy for pupil use of ICT**  
**February 2014**

(to be reviewed in [February 2015](#))



<b>Contents</b>	<b>Page</b>
<b>Introduction</b>	
<b>Scope of Policy</b>	
<b>Schedule</b>	<b>3</b>
<b>Responsibilities</b>	
<b>E safety Committee</b>	
<b>Internet use and AUPs</b>	<b>4</b>
<b>Photographs and videos</b>	
<b>Photographs and videos taken by parents/carers</b>	
<b>Mobile phones and other devices</b>	
<b>Use of e-mails</b>	<b>5</b>
<b>Security and passwords</b>	
<b>Data storage</b>	
<b>Reporting</b>	<b>6</b>
<b>Infringements and sanctions</b>	
<b>Rewards</b>	<b>8</b>
<b>Social networking</b>	
<b>Cyberbullying</b>	<b>9</b>
<b>Education</b>	<b>10</b>
<b>Monitoring and reporting</b>	<b>11</b>
<b>Appendix 1 – AUP’s</b>	<b>12</b>
<b>Appendix 2 – Parents letter concerning internet use</b>	<b>18</b>
<b>Appendix 3 – Audit</b>	<b>19</b>
<b>Appendix 4 – Photo permission form</b>	<b>20</b>
<b>Appendix 5 – Useful links</b>	<b>21</b>
<b>Appendix 6 – Shropshire Council Staff e-safety policy</b>	<b>22</b>

## Introduction

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of e-Safety;
- work to empower the school community to use the Internet as an essential tool for life-long learning.

This policy is used in conjunction with other school policies.

This policy has been developed by a working group which included representatives from all groups within the school.

## Scope of policy

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

## Schedule

The Implementation of the e-Safety policy will be monitored by an e-Safety working group, reporting to the Governors annually.

The e-Safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to e-Safety or incidents that have taken place.

The e-Safety policy approved by Governing body on \_\_\_\_\_

Signature of Chair of Governors: \_\_\_\_\_

The next review date is: \_\_\_\_\_

## Responsibilities

The member of SLT team responsible for e-safety is	Chris Ball
The governor responsible for e-safety is	Frank Bury
The e-safety co-ordinator is	Susan Rook

## 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. 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

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 lessons in 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.

The Consent form used is in appendix 4.

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.

### **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**

Pupils' mobile phones will be confiscated and sent straight to the school office in a sealed envelope that has the pupil name and class written on. Confiscated phones can be collected by parents/carers at the end of the school day.

### **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.

## **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 ICT reporting book that is kept in the general office. 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 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)

## 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.

### 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 / confiscation of phone / 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:

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

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

### **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.

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.

### **Rewards**

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. Above and Beyond, class and individual commendation for good research skills and for being good cyber citizens etc.



## Social networking

Pupils are not permitted to use social networking sites within school. See the separate School staff e-safety policy for guidance on staff use of social media.

## Cyberbullying

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

- The school will follow procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:
  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP.
  - Parent and carers of pupils will be informed.
  - The police will be contacted if a criminal offence is suspected.

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

### **Parents and the wider community**

Parents, carers, etc can obtain any additional information and advice or training resources on e-safety from the School on request.

## **Monitoring and reporting**

- a). 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
- b). The records are reviewed / audited 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.

## **Appendices**

### **Appendix 1 – AUP's**

# AUP for learners in the Foundation Stage and KS1

*This is how we stay safe when we use computers:*

I agree that I will:

- ask a teacher or suitable adult if I want to use the computers
- always keep any passwords a secret
- only use activities that a teacher or suitable adult has told or allowed me to use
- take care of the computer and other equipment
- ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- tell a teacher or suitable adult if I see something that upsets me on the screen
- only open pages which my teacher has said are OK
- 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)
- never agree to meet a stranger
- 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
- only use my school email
- only email people I know or if my teacher agrees
- I know that if I break the rules I might not be allowed to use a computer

*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 (child):.....

## **AUP 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:

- take care of the computer and other equipment
- ask a teacher or suitable adult if I want to use the computers
- always keep any passwords a secret
- only use activities that a teacher or suitable adult has told or allowed me to use
- ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- tell a teacher or suitable adult if I see something that upsets me on the screen
- only open pages which my teacher has said are OK
- 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
- never use my own mobile device in school unless I am given permission
- never give my phone number to others on the internet
- only email people I know or approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- never use of a social networking site at school
- 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 (child):.....

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

***Signed*** \_\_\_\_\_



## **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

# **Corvedale CofE Primary School Parent E-Safety Consent Letter**

**Parent / carer 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 at school. 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

I am aware that publication of defamatory comments on the internet, via social media and other online forums, about members of the school staff or governors can potentially be libellous.

**Parent's signature:**..... **Date:**.....

## Appendix 3 – School audit

### Audit

The self-audit in should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Shropshire guidance?    Yes/No

Date of latest update (at least annual): \_\_\_\_\_

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 e-Safety Policy was approved by the Governors on \_\_\_\_\_

The policy is available for staff at: \_\_\_\_\_

The policy is available for parents/carers at: \_\_\_\_\_

## Appendix 4 – 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/SLG?               | 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 |

Signature:

Date:

Your name (in block capitals):

## **Appendix 5 – Links**

### **(a) Shropshire Council Education Improvement Service documentation**

All EIS 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>

## Appendix 6

Shropshire Council has developed an e-safety policy for school staff which has been agreed by the following Professional Associations / Trade Unions representing staff in schools:-

- National Union of Teachers
- National Association of Schoolmasters Union of Women Teachers
- Association of Teachers and Lecturers
- National Association of Head Teachers
- Association of School and College Leaders
- UNISON
- GMB

The policy can be found at:

<https://www.shropshirelg.net/services/hr/noticeboardnews/Documents/E-Safety%20Policy.pdf>

## Sanctions for misuse: Pupils

Schools should populate the grid below marking appropriate possible sanctions. Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore ticks may appear in more than one column. The ticks in place are actions which must be followed

Incidents:	Refer to class teacher / tutor	Refer to Head of Department /	Refer to Headteacher	Refer to Police	Refer to technical support staff for	Inform parents / carers	Removal of network / internet	Warning	Further sanction / en detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other handheld device									
Unauthorised use of social networking / instant messaging / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or									

sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									



## Sanctions/Actions Staff

Schools should populate the grid below marking appropriate possible sanctions. Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore marks may appear in more than one column. The marks in place are actions which must be followed.

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(	Refer to Technical	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).								
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email								
Unauthorised downloading or uploading of files								
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								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff								
Sending an email, text or instant message that is regarded as offensive, harassment or of a								

bullying nature to learners								
Breach of the school e-safety policies in relation to communication with learners								
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								