Tameside Safeguarding Children Board

e-safety Scaffold

Guidance on writing E-safety/acceptable use policies for schools and other agencies that work with children and families

Essential Explanatory note!

The ***e-safety Scaffold*** is a document to assist schools, agencies and organisations to write e-safety and acceptable use policies. From page 3 of this document you can lift the material and adapt as you decide is appropriate for your agency.

There are notes in the margins to help you decide whether the particular content is appropriate for your policy.

When drafting your e-safety and acceptable use policy you should also refer to the TSCB Guidance – ***Safeguarding Children Online.*** This provides principles of best practice and policy-making that you should consider when producing your e-safety and acceptable use policy.

You can also use the TSCB Guidance - ***Safeguarding Children Online*** to ensure that you have in place the correct systems and strategies for creating a safe environment for the use of electronic media.

It is very important to recognise that E-safety is not an ICT issue. It may involve the use of ICT but it is about protecting children and young people from harm. **If you have a concern about actual significant harm to a child or young person, or the risk of significant harm, then** you should immediately activate your own agency safeguarding children or child protection procedures, use the *TSCB Safeguarding Children Framework* and make a referral to Children's Social Care. Again this is no different to concerns in other situations. If a child or young person is in immediate danger then contact the Police on 999.

Useful Contact Numbers:

Children's Social Care Referral & Assessment Team: 0161 342 4186 / 4199 / 4222
Out of Hours: 0161 342 2222
LADO (Local Authority Designated Officer): 0161 342 4111
GM Police Public Protection Investigation Unit (PPIU): 0161 856 9314

TSCB website www.tamesidesafeguardingchildren.org.uk

Name of Establishment / Service

E-Safety/Acceptable Use Policy

Name of E Safety Officer in Organisation & Contact Details

Written by: XXXXXXXX

Date: XX/XX/XXXX

Date for review: XX/XX/XXXX

Introductory Statement

Open the policy with a short statement detailing the establishment's / service's view on the use of new technology, including the Internet. E.g.

- *The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.*
- *Use of email, mobile phones, Internet messaging, social networking sites and video hosting sites all enable improved communication, facilitate the sharing of data and resources and improve opportunities for socialising and communicating with people from around the world.*
- *Virtual Learning Environments (VLEs) provide children and/or young adults with a platform for personalised and independent learning.*

Mention how the dangers associated with the Internet and emerging new technologies are highly publicised in the media and highlight some notable examples. E.g.

- Children and/or young adults might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.
- Children and/or young adults might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as Facebook and video hosting sites such as Youtube etc.
- Young people may share personal and private images / information with somebody they consider a friend or boyfriend / girlfriend which at a later date is then shared online without their permission. Once posted online the image / information can be shared with a rapidly growing audience.
- Children and young people may be groomed online.

Point out that there are social and educational benefits to be derived, however. E.g.

- Children and/or young adults are equipped with skills for the future.
- The Internet provides Instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's and/or young adults' reading and research skills.
- Email, Instant messaging and social networking helps to foster and develop good social and communication skills.
- Children and young people can keep in contact with family and friends worldwide.

State the fact that these far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

Explain how this policy, written in accordance with BECTA guidelines, focuses on each individual technology available within the establishment / service and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

Comment [a1]: Note: Procedures for any new technology being introduced into the establishment / service must be added when the policy is reviewed. As technology is changing so quickly, the E-Safety Policy will therefore be subject to constant review and amendment. You should consider making it a requirement to write a risk assessment for any emerging technology which is to be introduced and used in the interim – see the 'Concluding Statement'.

Procedures for Use of a Shared Network

(N.B. This will not be applicable unless PCs in the establishment/service are networked).

In this section, you need to outline what users must and must not do when using a PC / laptop connected to a network. You may wish to consider the following statements and adapt them according to the context of your establishment/service.

- Users must access the network using their own logons and passwords. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should not be installed without prior permission from the person responsible for managing the network.
- Removable media (e.g. pen drives / memory sticks, CD-ROMs and floppy disks) must be scanned for viruses before being used on a machine connected to the network.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.

(N.B. If the establishment/service has a wireless network, it must be encrypted to prevent outsiders from being able to access it. This needs to be done and a procedure for ensuring that this is securely maintained and for outlining how passwords will be kept safe must be included in the E-Safety policy).

Procedures for Use of the Internet and Email

Outline the procedures for safe Internet and Email use as agreed by the establishment/service. NOTE: Each individual establishment/service must decide these for itself based upon their own unique context. A generic template will not suffice as every establishment/service is different and some of the statements below will not apply to all. You may wish to consider the following examples when drawing up your procedures and tailor them to suit your establishment/service circumstances.

Comment [a2]: N.B. If the establishment/service has 'guest users' from time to time, you might consider setting up a generic password for them. The statement would then need to be adjusted to reflect this.

Comment [a3]: Your policy should name the person responsible for this. If there are any exceptions to this rule, they need to be pointed out here.

Comment [a4]: You will need to outline procedures for how this will be carried out.

- All users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.
- Parental or carer consent is *requested** in order for children to be allowed to use the Internet or email.
- Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.
- The Internet and email must only be used for professional or educational purposes.
- Children must be supervised at all times when using the Internet and email.
- Procedures for Safe Internet use and sanctions applicable if rules are broken will be clearly displayed beside every computer with access to the Internet.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the person responsible for E-Safety and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
  (N.B. You will need to find out exactly what is in place before you can state this in your policy).
- Internet and email use will be monitored regularly in accordance with the Data Protection Act.
- Email addresses assigned to individual children will not be in a form which makes them easily identifiable to others.
- Users must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All emails sent from an establishment/service email account will carry a standard disclaimer disassociating the establishment/service and the Local Authority with the views expressed therein.

Comment [a5]: It should also apply to any 'guest users' as they need to know what is and what is not acceptable and sign to show their agreement to abide by the rules before access is permitted.

Comment [a6]: *This is not statutory, though advisable to cover the establishment/service in case any incident of abuse or misuse occurs. It is also a way of highlighting safe Internet practices and behaviours to parents who might then reinforce these at home.

Comment [a7]: This will depend on the setting of the establishment and will also depend on the age and development of the child / young person.

Comment [a8]: You will need to name this person.

Comment [a9]: You need to state who is responsible. E.g. Network manager, technician, E-Safety Officer, etc. They must be supervised by a senior member of staff when this is done, however. It is vital that this is mentioned in this E-Safety policy and adhered to. An establishment/service may wish to make random spot checks or carry out more timetabled checks. This should be clearly explained in the policy and it must be drawn to the attention of all staff and Internet users. Some users may argue that this violates individual rights, etc. If they have been well informed that checks will be made in accordance with data protection law and they have signed an acceptable use agreement, they have thereby consented to this checking process.

Comment [a10]: N.B. This point is extremely important. If an email address contains a child or young person's name and the establishment/service name, others could guess an email address and that individual might then become a target for 'cyber-bullying' or they may receive unwanted / spam emails.

Comment [a11]: In some cases, children and/or young adults might be required to register in order to log into an educational site or a social networking site approved by the establishment/service. In this case, it might be advisable to state in the rules that 'cyber names' (pseudonyms) must be used, which will not allow them to be identified.

- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the service / establishment. Emails received should not be deleted, but kept for investigation purposes.

- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

- All email attachments must first be scanned before they can be opened.

- Users must seek permission before downloading any files from the Internet.

- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

Comment [a12]: You must check that this is the case or it will invalidate the statement..

Comment [a13]: It may be that the email system in the establishment/service already does this, but if not, this is important. You might also want to restrict this further and decide that any emails with attachments received from unknown senders, and / or if the content of an attachment is not detailed in the body of an email, it should not be opened, but subsequently deleted. If so, you must state this clearly in your policy.

Comment [a14]: There will be opportunities to do this in some settings. In other establishments, however, posters might need to be used in computer bays / areas to inform users of this.

Procedures for Use of Instant Messaging (IM) and Social Networking Sites

Outline the procedures agreed by the establishment/service regarding the use of IM and Social Networking Sites. You might wish to block their use outright, though depending on what establishment / service you work within, this may not be desirable. You might instead allow these to be used, having educated users on safe practices and behaviours, or impose some restrictions on their use.

If you decide on an outright ban, the following statements might be included in your policy:

- The use of Instant messaging (e.g. MSN messenger) is not permitted

- Use of social-networking websites e.g. Facebook is not permitted.

- Children/Young adults and staff must not access public or unregulated chat rooms.

If the context of your establishment / service dictates a more lenient approach, then the following statements are worth consideration and might, with some amendment, be included in your policy:

- Children/young adults and staff are permitted to join in forums which are moderated and hosted by a respectable organisation or to access regulated chat rooms.

- Use of weblogs is permitted. This will be supervised and children / young adults will be reminded of the safe practices and behaviours to adopt when posting material, as well as the need to adopt a formal and polite tone at all times.

Comment [a15]: You might restrict this to educational purposes only.

- The establishment/service recognises that children/young adults need to be allowed the freedom to use Instant Messaging, social-networking websites and weblogs, but aims to educate them into adopting safe practices, whilst promoting awareness of the dangers of these new technologies, so that they are equipped to make their own assessment of risk.

Comment [LCJ16]: It would be useful to involve young people in developing a code of conduct of expected behavior whilst using IM and SN sites which should include a statement about what to do if somebody breaks this code of conduct.

Procedures for Use of Cameras, Video Equipment and Webcams

Outline the procedures for safe use of photographic and video equipment as agreed by the establishment/service. As above, each individual establishment / service must decide these for itself based upon its own unique context. You may wish to consider the following examples when drawing up your procedures and tailor these to suit. N.B. The points in BOLD need to be included in your policy, though these can be reworded and added to.

- **Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. Permission requests should explicitly state where photographs / video images will and will not be displayed – especially if these will be online.**

Comment [a17]: This must be done where children are concerned. Parents / carers need to be able to give informed consent and therefore need information as to what images will be used for and where they will be displayed.

- Staff should use a designated work camera / video for any photographic / video footage.
- Photographs or video footage will be downloaded immediately and saved into a designated folder. This will be password protected and accessible only to authorised members of staff.
- Any photographs or video footage stored must be deleted immediately once no longer needed.
- Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a 'password-protected' folder on an establishment/service computer immediately upon their return.

Comment [a18]: To protect staff, some schools have decided not to allow teachers to use personal cameras and camera phones, but again, this might not be appropriate for your establishment or service.

- Children / Young adults should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.
- Webcams must not be used for personal communication and should only be used with an adult present.

Comment [a19]: In some settings, however, it might not be appropriate to ban this, but safe practices must be established before use is permitted and these should be outlined in your policy.

- Children / Young adults and staff must conduct themselves in a polite and respectful manner when representing the establishment/service in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

- Digital images should not be uploaded onto any sites which include 'tagging' facilities e.g. facebook as a name can be attached to a child exposing their identify and this image can also be shared with other people without permission.

- If images are displayed online care names should not be attached to the image.

Procedures to ensure safety of the establishment's / service's website

If an establishment/service has its own website, then it is important that measures are in place to ensure the safety of children / young people and staff represented on this. The following guidance needs to be considered when drawing up acceptable use statements. N.B. As previously, the points in BOLD need to be included in your policy, though these can be reworded and added to.

- The establishment/service should have a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.

- The establishment/service website should be subject to frequent checks to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.

- **Copyright and intellectual property rights must be respected.**

- **Permission must be obtained from parents or carers before any images of children can be uploaded onto the establishment/service website.**

- **Names must not be used to identify individuals portrayed in images uploaded onto the establishment/service website. Similarly, if a child / young person or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.**

- **When photographs to be used on the website are saved, names of individuals should not be used as file names.**

  Important to note*: It is sensible to outline this as a procedure in the E-Safety policy and to discuss this with staff as this is something which people would often not think twice about doing. If the photographs are not stored in a 'password-protected' folder, individuals can be easily identified or if photographs are uploaded onto a website or downloaded, the file names may be visible.*

- If the establishment/service website contains a Guestbook, public noticeboard, forums or weblogs, these must be monitored regularly to check that no personal information or inappropriate or offensive material has been posted.

Comment [a20]: You might mention who will carry out these checks and how frequently

Comment [a21]: It is important that permission is granted before any files created or owned by another person or company are used. This will most certainly apply to photographs, graphics, animations, audio and video clips, clips from TV shows such as those on 'YouTube,' scanned images from books, newspapers or magazines, etc. Legal action can be taken if this is contravened.

Comment [a22]: You might decide not to publish images of individuals, but insist on using group photographs only. If so, you must mention this in your policy.

Comment [a23]: Your policy will need to point out who will be responsible for checking this and how often it will be done. Also, what will be done if any personal information or inappropriate content appears? I.e. Will it be deleted immediately? Will any further investigation be needed? Will any abuse or misuse be recorded? And if so, by whom?

Procedures for using mobile phones and Personal Digital Assistants (PDAs)

Each establishment/service should have its own rules already in place for mobile phones (particularly camera phones) and portable handheld devices.

The following points need to be considered when drawing up acceptable use statements.

- Would children / young adults (and staff) be required to switch mobile phones off at particular times? These must be outlined in your policy and made explicit to users.

- The taking of still pictures or video footage without the subject's permission is not ethical, so rules would need to be in place to protect the individual.

- Some individuals might use a mobile / camera phone for inappropriate or malicious purposes. I.e. for 'happy-slapping,' the sending of abusive or unsavoury images / text messages, the making of hoax, crank or abusive phone calls, etc. How would you deal with this? How would such instances be reported and dealt with? How would you prevent this from happening? I.e. educating children, young adults, parents and staff. Courses of action will need to be agreed, shared with all concerned and detailed in your policy.

- What must children / young adults and staff in your establishment / service do if they receive unwanted or hurtful calls or text messages? (N.B. Any such messages should not be deleted nor replied to. This would need to be pointed out). Similarly what should individuals do if contact is made by a person unknown to them?

- It is very easy for individuals to access inappropriate websites and content via mobile phones and PDAs nowadays. Rules would need to be in place to discourage this and to deal with any violation. Education again is key. Note: This is very difficult to police as you cannot impose filters on content viewed or downloaded on an individual's mobile phone.

Procedures for using wireless games consoles

In some settings, a ban on wireless games consoles might be the most appropriate course of action. Not only might they lead to instances of theft, but as children can also connect to the Internet and play against other people online, they represent the same dangers as public chat rooms. If these are to be permitted, however, the following points need to be considered.

- When will their use be permitted?

- Will children be allowed to play online? It may not be such an issue with young adults, but there is still a duty to inform users about the dangers of giving out any

personal information which might help to identify them. They should use a 'cyber-name' where any registration is required.

- Any unwanted contact received via a wireless games console, which makes children or young adults feel vulnerable or uncomfortable, must be reported immediately to a trusted adult.

Procedures for using Portable media players (e.g. iPods)

Again, the establishment/service may wish to ban their use to avoid instances of theft or damage. If it is not appropriate or possible to do so, the following points need to be considered when drawing up your policy.

- When will their use be permitted? E.g. At break times only; for downloading and listening to educational podcasts; for general use. i.e. listening to music and watching videos, etc. This needs to be made explicit in your policy.

Sanctions to be imposed if procedures are not followed

You may wish to detail the steps to be taken if rules are broken and/or the types of sanctions the establishment/service intends to impose if procedures are not adhered. e.g.

- Disciplinary action against staff
- Letters may be sent home to parents or carers (if applicable).
- Users may be suspended from using the establishment's /service's computers, Internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

You may wish to include a brief statement explaining that cases of misuse will be considered on an individual basis by a named person (s) and sanctions agreed and imposed to 'fit the crime.'

Concluding Statement

You need to mention that you are aware that the procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the establishment/service and that this policy will not remain static. It may be that staff / young adults / children might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

Comment [a24]: You will need to decide upon and name the person, who will be responsible for approving any risk assessments submitted.

Appendix

i. Acceptable Use Agreement for Staff

ii. Acceptable Use Agreement for Pupils / Young adults

iii. Acceptable Use Agreement for Guest Users

iv. Risk Assessment Proforma for Emerging Technologies

Comment [a25]: See example AUP for a Secondary School Staff attached. Note: This is not a generic copy to which a school or service should merely insert their name, however! This can be adapted by any school/organisation or service for young people.

Comment [a26]: See example AUP for a Secondary School attached. Note: This is not a generic copy to which a school or service should merely insert their name, however! This can be adapted by any school/organisation or service for young people.

Comment [a27]: These will be like short contracts listing what is / is not acceptable. They should be signed and dated.

Comment [LCJ28]: Please see attached risk assessment pro forma which could be adapted for the organisation's purposes.

Appendix 1 – **Example of an ICT Acceptable Use Policy (AUP) for staff and Young People.**

Name of organisation

ICT ACCEPTABLE USE POLICY DOCUMENT

Date:

E Safety Coordinator:
Name:
Contact Details:

Name of organisation

I.C.T. Acceptable Use Policy

---

1. Introduction

As use of the internet by staff and volunteers becomes more widespread, for the protection of the organisation, young people and the staff and volunteers it is necessary to set out some guidelines for internet use. Staff and volunteers should read these guidelines carefully, in conjunction with the organisation ICT Security Policy. Abuse of the internet may lead to disciplinary action being taken.

The use of electronic communication and information retrieval is no more than the addition of another medium. **The same behavioural and professional standards are expected of staff and volunteers as are the case with traditional written communications, the telephone and face to face meetings.**

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and developments of the internet itself.

Please Note: The following acceptable use policy refers to ICT use for staff in a school – this would need to be adapted dependent on the setting and how and when staff have access to the internet. The TSCB E Safety Scaffold will help you to write an AUP specifically for your establishment.

2. Acceptable Uses

As a general principle, internet access is provided to staff and volunteers to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the organisation considers to be acceptable uses of the internet:

- To provide communication within the organisation via email or the organisation website
- To provide communication with other organisations for educational purposes
- To distribute electronic copies of the weekly bulletin and newsflash
- To distribute details regarding organisation meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

3. Unacceptable Uses

The following uses will be regarded as not acceptable:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- Use of non-educational games.
- To access pornographic, obscene or illegal material.
- To solicit personal information with the intent of using such information to cause harm.
- Entering into a commitment on behalf of the organisation (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about the organisation, your colleagues and/or our young people on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information about the organisation in a personal online posting, upload or transmission - including financial information and information relating to our young people, staff and/or internal discussions
- Use of personal email to communicate with or about any MHHS students
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet.
- Use of any Bit torrent systems
- Use for personal or private business purposes.

4. Netiquette

The following general principles should be adopted:

- Be polite. Do not be abusive in messages to others.
- Use appropriate language. Remember that you are a representative of the organisation and that you are using a non-private network.

5. Email

- Whenever e-mail is sent, it should be from an official work email address which includes the sender's name, job title and organisation's name..
- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.

- If you receive e-mail from outside the organisation that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the organisation's guidelines).
- You should be aware that, in the event of the organisation being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Email should be accessed via organisation ICT equipment only, if you wish to use a personal device to download organisation emails, you must check with your line manager first. You will need to ensure that your device is secured by a password at all times, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.

6. Social Networking Sites

Social media applies to blogs, microblogs like Facebook, Twitter, Bebo, LinkedIn, videos, MySpace, social networks, discussion forums, wikis, and other personal webspace. This organisation permits the use of internet and social media on work premises, outside of work time, but only where it meets the following guidelines. This is usually outside normal working hours and must not interfere with your or others day-to-day duties. Personal access should not be in view of any young people, and you are reminded to log out or 'lock' the screen immediately upon leaving your mobile phone or PC, even if only for a short while.

- Do not "speak" for the organisation unless you have express permission to do so, this covers all comments relating to the organisation
- Protect yourself from identity theft
- If you can be linked to the organisation, act appropriately. This includes photos and status updates
- Remember that colleagues, prospective employers, parents and children may see your online information
- The organisation policy is that you are not allowed to be 'friends' with young people with whom you work or have worked with in the past unless there are exceptional circumstances, e.g. child, sibling etc
- Please choose your 'friends' carefully, especially in light of the last above. Ensure your settings are on private and only you and YOUR friends can see them.
- If in doubt, please seek advice in organisation.

7. Disciplinary Action

Disciplinary action may be taken against staff and volunteers who contravene these guidelines, in accordance with the organisation's disciplinary procedures.

8. Advice

If you require any advice on the use of these guidelines, please contact your Line Manager.

I have read and agree to abide by the rules stated in the I.C.T. Acceptable Use Policy. I understand the consequences if I do not.

Name: _____ **Job Title:** _____

Signed: _____

_____ **Date:** ___

_____

Appendix 11 – **Example of an ICT Acceptable Use Policy (AUP) for staff and Young People.**

Information and Communications Technology
Acceptable Use Policy

Young People's Guidelines for Internet Use

General

Young people are responsible for good behaviour on the internet just as they are in a classroom, a library or any public space. The general rules of behaviour expected by *(insert name of organisation)* apply for this too.

Please Note: The following acceptable use policy refers to ICT use in a school – this would need to be adapted dependent on the setting where the young person is accessing the internet and the age and development of the young person. The TSCB E Safety Scaffold will help you to write an AUP specifically for your establishment.

The internet is mainly provided for you to do research, access the VLE and backup your work. Your parents/carer's permission is required before you are allowed to use it though and there is space at the bottom of this for them to sign. Remember the motto: "Access is a privilege, not a right" and that access requires responsibility.

When you access the computer system in organisation and the internet, you will be given your own username and password. You are responsible for your behaviour and any communications (email, SNS etc) you have over the network. You must comply with organisation standards and honour this agreement that you will sign.

Your computer storage area (My Documents) will be treated like your organisation lockers. In the interest of your safety, we may review files and communications to ensure that you are using the system responsibly. This means that you should not expect that files stored on servers or storage media are always private.

During lessons, teachers will guide you towards appropriate materials. Outside of organisation, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted within the organisation:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others (cyber bullying)

4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords or accounts
7. 'Hacking' into others' folders, work or files for any reason.
8. Intentionally wasting limited resources, including printer ink and paper.

Sanctions

1. If you break any of the above rules, you may receive either a temporary or permanent ban on your internet/computer use.
2. Your parents/carers will be informed.
3. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour, including cyberbullying.
4. If necessary, police or local authorities may be asked to get involved.
5. If necessary, external agencies such as Social Networking or Email Member sites may be contacted and informed.

Insert Name of Organisation:

Information and Communications Technology
Acceptable Use Policy

Young people

- You must have your parent's / carer's permission before using the internet.
- You must have a supervising member of staff with you at all times when using the internet.
- Do not tell anyone your password or login name, other than the persons responsible for running and maintaining the system.
- Do not upload/send personal addresses, telephone / fax numbers or photographs of anyone (*staff or pupil*) at the organisation wither through email or SNS.
- Do not download, use or upload any material which is copyright. Always seek permission from the owner, before using any material from the internet. If in doubt, do not use the material. This includes downloading videos and songs.
- Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material of a violent dangerous or inappropriate context. If you are unsure ask your teacher
- Always respect the privacy of files of other users.
- Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Report any incident which breaches these rules to your teacher or a trusted adult in organisation.

Appendix 1V Risk Assessment Pro forma for Emerging Technology

Name of Staff member in Charge:_____

Date submitted: _____

Details of technology planned to be used.

_____
_____
_____
_____

Details of activity

_____
_____
_____
_____

Which pupils / young people will be involved?

_____
_____
_____

Which other members of staff will be involved?

_____
_____
_____

PASS / REVIEW / REFUSAL Date of decision _____

REVIEW

Reason for Review:

_____
_____
_____

Date of Review: _____

Outcome of review PASS /REVIEW /REFUSAL

_____
_____
_____