CLARENDON ROAD PRIMARY SCHOOL

ONLINE SAFETY & MOBILE TECHNOLOGY POLICY

Approved by:		**Date:**	
Last reviewed on:	*March 2019*		
Next review due by:	*March 2020*		

RELEVANT GUIDANCE

Project Phoenix - Positive Relationships and Online Safety: Guidance for Primary Schools

RELATED CHAPTERS

E-Safety Working Practices for Staff Procedure

Useful Guidance for Schools – Sex and Relationships Education

Contents

1. Introduction
2. What Are We Talking About?
3. Key Strategic Objectives for Online Safety
4. Promoting a Safe Environment for Children using Electronic Media
5. Responding to Concerns About the Safety of Children and Young People
6. Responding to Concerns About the Online Conduct of Staff and Volunteers
7. Safer Working Practices for Those Working or Volunteering with Children
8. Sexting - Self Generated Explicit Images of Children and Young People
9. Useful Websites
10. Additional Local Information

Appendix 1: Example of an ICT Acceptable Use Policy (AUP) for Staff and Young People

Appendix 2: Example of a Standards of Proficiency Written for All Staff (Paid /Unpaid) When Using Online Communication

1. Introduction

1.1 Every child and young person should be able to participate in an enjoyable and safe environment and be protected from abuse and these same principles apply in the online environment. This is the responsibility of every adult.

1.2 The Internet offers tremendous benefits and opportunities for children and young people and this procedure is certainly not intended to curtail any potential for fun, entertainment and learning. However, as with any social space, using the internet will pose some risks for children and young people particularly if they are unaware of the way that information / technology can be used by others (children / adults) with ill-intent to exploit or abuse them.

1.3 Child abuse is a very emotive and difficult subject for everyone involved. When the abuse / harm occurs online it can be even more challenging because many people who are significant in the child's life may not be as knowledgeable about the technology used. Indeed it is likely that the child or young person may know more than the adults around them about how to use the technology.

1.4 A child could experience abuse/harm online without actually ever meeting the person causing the harm in 'real life'. The abuser could also remain anonymous or adopt a pseudo identity.

1.5 Young people may be worried about confiding in adults about concerns or worries about things happening to them online through fear of the adult over reacting and / or confiscating their treasured device as an ill informed method of safeguarding that child.

1.6 It is important to remember it is not the technology itself that is the source of harm but rather the behaviour of another person that causes harm whilst online. Confiscating a particular device is therefore not an appropriate response to safeguard a child from harm online. The arrangements in response to harm/potential harm experienced online should be same as the arrangements in response to harm experienced by a young person in the 'real world'.

2. What Are We Talking About?

2.1 When this policy refers to 'online', this means somebody using a device to gain access to the Internet. How somebody accesses the Internet or 'gets on line' will vary massively especially as technology is changing so rapidly; the list below is a starting point of different means of getting online. However this is certainly not exhaustive and will change over time:

- Computers, PCs, Laptops, iPads, Personal Digital Assistants (PDAs) etc;
- Mobile phones, Smartphones, 3G phones etc;
- Through WiFi connections available in restaurants, cafes, hotels etc;
- iPods, MP3s etc;
- E-mail, Instant messaging, Texts, Blackberry Messenger;
- Social networking sites e.g. Facebook, Twitter;
- Video hosting websites e.g. Youtube;
- Games consoles e.g. Xbox Live, PlayStation Network, Nintendo Online;
- Chatrooms and Blogs;
- Webcams.

2.2 All agencies providing Internet access to children and young people should have an Acceptable Use Policy, which sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of online technologies. Tameside LSCB has developed an **E-Safety Scaffold** to support organisations in developing acceptable use policies for children and young people, staff and parents/carers when using equipment with access to the Internet in their establishment.

2.3 An example of an ICT Acceptable Use Policy for staff and young people (AUP) can be found in **Appendix 1: Example of an ICT Acceptable Use Policy (AUP) for Staff and Young People.**

3. Key Strategic Objectives for Online Safety

3.1 Byron (2008) classifies the online risks to children in terms of content, contact and conduct. Byron goes on to say that to reduce risks means achieving three objectives:

Objective 1: Reduce Availability

Reduce the availability of harmful and inappropriate content, the prevalence of harmful and inappropriate contact and the conduciveness of platforms to harmful and inappropriate conduct;

Objective 2: Restrict Access

Equip children and their parents to effectively manage access to harmful and inappropriate content, avoid incidences of harmful and inappropriate contact and reduce harmful and inappropriate conduct;

Objective 3: Increase Resilience

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

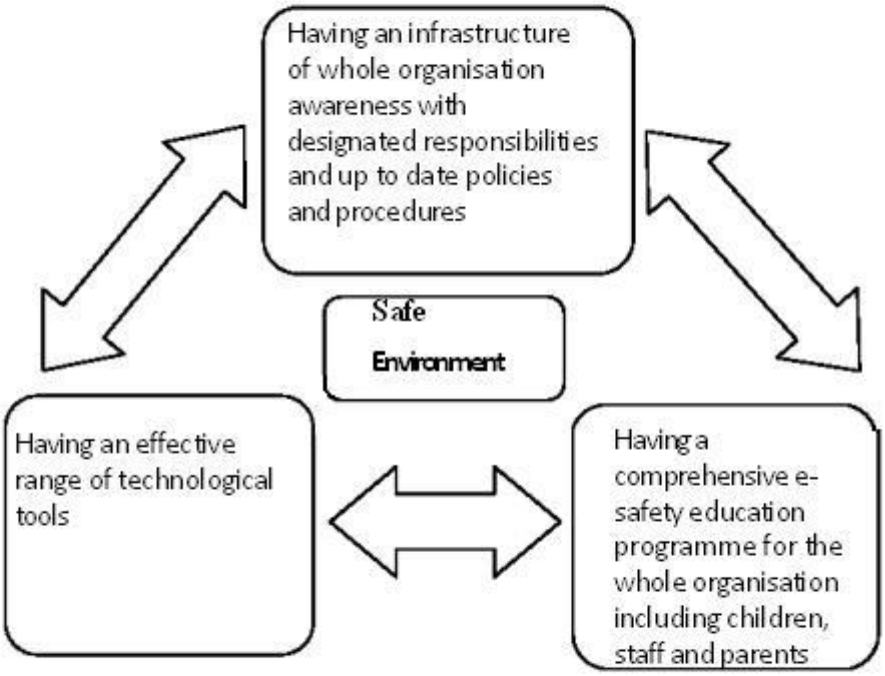
3.2 Therefore any e-safety policy should address these strategic objectives.

In particular, the third objective is very important. If children and their parents can be empowered to safely manage the availability of and access to harmful contact, content and conduct then it will be less necessary for agencies to impose restrictions on availability and access.

4. Promoting a Safe Environment for Children Using Electronic Media

4.1 Creating a safe environment for the use of electronic media is as much about a safe working culture and practices as it is about putting into place technical safeguards.

4.2 There are 3 components to creating a safe environment:



Having an infrastructure of whole organisation awareness with designated responsibilities and up to date policies and procedures

Safe Environment

Having an effective range of technological tools

Having a comprehensive e-safety education programme for the whole organisation including children, staff and parents

The following questions are helpful to assess how e-safe your organisation is:

Does your organisation........

1. Have a nominated e-safety coordinator?
2. Have the necessary acceptable use policies?
3. Check that appropriate e-safety procedures and practices are in place and working?
4. Use an accredited supplier for internet services?
5. Include e-safety as part of your inspection evidence?
6. Keep a log to record and monitor e-safety incidents?
7. Raise awareness of e-safety issues by holding workshops and events?

Do all your staff and volunteers........

1. Understand e-safety issues and risks?
2. Receive regular training and updates?
3. Know how to support youngsters with new technologies?
4. Know how to report and manage issues or concerns?
5. Know how to keep data safe and secure?
6. Know how to protect and conduct themselves professionally online?
7. Take the opportunity to consult with children and young people?

Do your children and young people........

1. Understand what safe and responsible online behaviour means?
2. Get opportunities to learn about e-safety?
3. Get the opportunity to improve their digital literacy skills, e.g. how to search safely and effectively online?
4. Know the **SMART** (Safe, Meeting, Accepting, Reliable, Tell) rules?
5. Get the opportunity to give their views about staying safe online?
6. Know how to report any concerns they may have?

Can your parents and carers........

1. Understand e-safety issues and how to manage risk?
2. Understand their roles and responsibilities?
3. Receive regular training and updates?
4. Understand how to protect their children in the home?

5. Responding to Concerns About the Safety of Children and Young People

5.1 When there are concerns about the welfare of a child which have occurred online then the agency should use its usual safeguarding children procedures and good practice to respond to these. **In this sense the context of the abuse / harm occurring online is no different to other situations where there is a concern about a child's welfare**.

5.2 If there is a concern about actual **Significant Harm** or the risk of Significant Harm to a child arising whist online then the agency should immediately activate its own safeguarding children or child protection procedures, and make a referral to Children's Social Care - see **Making Referrals to Children's Social Care Procedure**. 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.

5.3 When an incident raises concerns both about Significant Harm and unacceptable use, the first and paramount consideration should always be the welfare and safety of the child directly involved.

5.4 To assist Police in any subsequent investigations, where possible, staff who are made aware of online abuse or inappropriate activity should try to preserve copies or records of offending material and obtain any relevant passwords to accounts or websites, where possible.
Suspected online terrorist material can be reported through **www.gov.uk/report-terrorism**. Reports can be made anonymously, although practitioners should not do so as they must follow the procedures for professionals.
Content of concern can also be reported directly to social media platforms – see **UK Safer Internet Centre, Social media help website**.

6. Responding to Concerns About the Online Conduct of Staff and Volunteers

6.1 If staff (paid/unpaid) behave in ways online that cause concern then this will usually be dealt with under the auspices of the Acceptable Use Policy or Standards of Proficiency of the agency (see example of an acceptable use policy in **Appendix 1: Example of an ICT Acceptable Use Policy (AUP) for Staff and Young People** and a Standards of Proficiency for online communication in **Appendix 2: Example of a Standards of Proficiency Written for All Staff (Paid /Unpaid) When Using Online Communication**). Acceptable Use Policies define what behaviour is acceptable when using digital technology and should be in place to help everyone understand all aspects of their duties when technology is involved.

6.2 However, if the conduct by staff or volunteers amounts to a concern about an abusive relationship with, or harmful behaviour towards, a child or young person then the **Managing Allegations of Abuse Made Against Adults Who Work with Children and Young People Procedure** should be followed.

7. Safer Working Practices for Those Working or Volunteering with Children

Everyone who works with children and young people, whether in a voluntary or paid capacity, must always have their professional role in mind whenever they are operating in the digital world.

E-Safety Working Practices for Staff Procedure sets out good practice guidelines when working with children and young people.

8. Sexting - Self Generated Explicit Images of Children and Young People

8.1 There have been an increasing number of incidents where young people have shared sexual images of themselves (referred to as 'sexting'). Where this happens, images have usually been shared with a partner or intended partner as a form of flirtation or - in the eyes of the young person - 'safe sex'. Sometimes this is as a result of pressure, however.

8.2 Whatever had prompted the sending of the image, the act itself poses a risk to the young person in the image: once it has been shared it is liable to be distributed further. The young person is then exposed to risk of high-level bullying and to the possibility of being stalked by a paedophile who has become fixated on them after finding the image online.

8.3 Young people of an age likely to consider such actions should be educated about the risks.

8.4 Any incidents that come to light should be handled carefully, bearing in mind both that possession of the images may constitute an offence in itself, and the child or young person whose image has been shared is at risk and may already be subject to an exploitative relationship.

8.5 There have been a number of cases of images or video of children or young people under the age of 16 engaging in sexual activity being shared. These are legally images of child sexual abuse, even if they have been shared by others of the same age. All such cases are evidence of a child or young person being sexually exploited and should be dealt with as such.

8.6 If images or video of children engaged in sexual activity or in revealing poses are known to have been posted online, the following guidelines should be followed:

- The Police should be contacted immediately. The police will be in a position to make judgments about how matters are pursued in relation to offences and offenders;
- The nominated person for child protection/safeguarding should initiate a CAF. Through the CAF process judgments will be made about the best means of supporting the child;
- Sites or networks on which the images appear should be alerted to the existence of illegal material. It is important that material online be removed as soon as possible, but staff must not put themselves at risk of illegality. Once the matter has been reported to the police their advice on this must be followed;
- Any young people who have themselves posted potentially illegal material should be told to remove the items, and warned that police action may follow if they do not. Through the CAF process, parents may also be involved;
- In some cases there may not be an obvious means of flagging or reporting the image (for example where a revealing picture of a young person has been used in an another young person's Blackberry Messaging profile). Even in these circumstances the existence of the image should be notified to the network provider (e.g. RIM for a Blackberry) and police action may be necessary to ensure its removal or engage the co-operation of the young person who has control of the image;
- The incident should be logged through the organisation's own monitoring / line management procedures;
- Appropriate educational/pastoral work should be undertaken with all young people involved.

9. Useful Websites

Suspected online terrorist material can be reported through **www.gov.uk/report-terrorism**. Reports can be made anonymously, although practitioners should not do so as they must follow the procedures for professionals. Content of concern can also be reported directly to social media platforms – see **UK Safer Internet Centre, Social media help website**.

Child Exploitation and Online Protection Centre (CEOP)

The Child Exploitation and Online Protection (CEOP) Centre is part of UK police and is dedicated to protecting children from sexual abuse wherever they may be. It provides a range of training and information resources and can be accessed at: **Child Exploitation and Online Protection Centre (CEOP)**.

thinkuknow

CEOP has a separate website for children, young people, parents, carers and practitioners and this gives advice on how children and young people can keep safe and in control when they are online. It also has information on how these groups of people can report concerns about harmful behaviour online. This can be accessed at: **thinkuknow**.

Internet Watch Foundation (IWF)

Inappropriate or harmful material online can be reported to the IWF. More details are at: **Internet Watch Foundation (IWF)**.

Childline

ChildLine is the free helpline for children and young people in the UK. Children and young people can call on 0800 1111 to talk about any problem - counsellors are always here to help you sort it out. See **Childline** website.

Childnet

Childnet mission is to work in partnership with others around the world to help make the Internet a great and safe place for children.

In all its work Childnet seeks to take a balanced approach promoting the positive and highlighting the creative and inspiring ways children and young people are using the medium for good. You can also read about the ways to respond to the negative aspects and dangers for children on the **Childnet** website.

Advice on Child Internet Safety

The Department for Education has published guidance for all organisations and Internet Service Providers (ISPs), compiled by members of the UK Council for Child Internet Safety (UKCCIS), on child internet safety. Issues covered include chatting online, sharing information online, gaming and networking.

'Munch, Poke, Ping'

'Munch, Poke, Ping' is a report produced for the UK Government's Training and Development Agency (TDA) in 2011. It considers the risks which vulnerable young people, excluded from schools and being taught in Pupil Referral Units (PRUs), encounter online and through their mobile phones. It considers what specific advice, support and safeguarding training staff working with these vulnerable young people need when it comes to understanding social media and mobile technology.

10. Additional Local Information

Click here to view Manchester Safeguarding Children Board's Policies and Resources website.

Appendix 1: Example of an ICT Acceptable Use Policy (AUP) for Staff and Young People

Click here to view Appendix 1: Example of an ICT Acceptable Use Policy (AUP) for Staff and Young People.

Appendix 2: Example of a Standards of Proficiency Written for All Staff (Paid /Unpaid) When Using Online Communication

Please Note: This Standards of Proficiency is not exhaustive and should be amended to reflect any additional expectations of staff and the age and development of the children / young people they are working with.

Adults who work with children and young people are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motives and intentions.

All communication by staff via any form of online communication will be for professional purposes only.

Any communication will be sent via a professional address only clearly showing the staff members name, job role and organisation.

All communication should acknowledge and maintain expected professional boundaries and be transparent and open to scrutiny.

Communicate with young people should be for professional purposes only.

Staff should not share their personal contact details with young people; this includes personal mobile numbers, email addresses, Social Networking profiles, Twitter accounts etc.

Staff should never accept a 'friend requests' from a young people or request a young people to be their 'friend'.

All staff are responsible for the security of their individual log-in and password and subsequently any communications sent from their address; they should not share their password and / or allow anybody else to log assuming their identity.

Any staff member who discovers their account has been hacked and / or their identity assumed should report this to their line manager.

All staff should record and report without delay any situation where they feel the actions of themselves / others (including young people) may have compromised the organisations or their own professional standing. Such incidents should be reported to their line manager.

Any member of staff concerned about the professional conduct of another member of staff should report this to their line manager in line with TSCB Procedure for Managing Allegations against Adults who work with Children and Young People.

Failure to comply with this Standards of Proficiency may result in disciplinary action.

Communication Devices and Methods

The following table shows the school's policy on the use of communication devices and methods. Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

Communication Method or Device	Adults	Pupils
Mobile phones may be brought to school	✓	✓ @
Use of mobile phones in lessons	☒	☒
Use of mobile phones in social time	✓	☒
Taking photos on personal mobile phones	☒	☒
Use of personal hand held devices e.g. PDAs, PSPs	☒	☒
Use of personal email addresses in school, or on network	☒	☒
Use of school email for personal emails	☒	☒
Use of chat rooms / facilities	☒	☒
Use of instant messaging	☒	☒
Use of social networking sites for school purposes	✓	☒
Use of internal school blogs	✓	✓

Key	
✓	Allowed
☒	Not allowed

@ Pupil mobile phones may only be on the premises with the consent of the Headteacher and with valid reason. Pupil mobiles should be switched off at all times.

Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school will monitor online activity using Smoothwall Web Filtering and Internet Safety system provided by RM. The school policy restricts certain internet usage as follows:

User Actions	Usage
Child sexual abuse images	☒☒
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation	☒☒
Adult material that potentially breaches the Obscene Publications Act in the UK	☒☒
Criminally racist material in UK	☒☒
Pornography	☒☒
Promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability	☒☒
Promotion of racial or religious hatred	☒☒
Threatening behaviour, including promotion of physical violence or mental harm	☒☒
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	☒☒
Using school systems to run a private business	☒
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school	☒
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions	☒
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)	☒
Creating or propagating computer viruses or other harmful files	☒
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet	☒
On-line gaming (educational)	⚠
On-line gaming (non educational)	☒
On-line gambling	☒
On-line shopping / commerce	⚠
File sharing	✓
Use of social networking sites	⚠
Use of video broadcasting e.g. YouTube	⚠
Accessing the internet for personal or social use (e.g. Online shopping)	⚠
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses	⚠

Key	
✓	Allowed
☒	Not allowed
☒☒	Not allowed and illegal
⚠	Allowed at certain times / with permission

Good Practice Guidelines

Email

Best Practice

✓DO✓

Staff and students/pupils should only use their school email account to communicate with each other

Safe Practice

⚠CHECK ⚠

Check the school Online Safety policy regarding use of your school email or the internet for personal use e.g. shopping

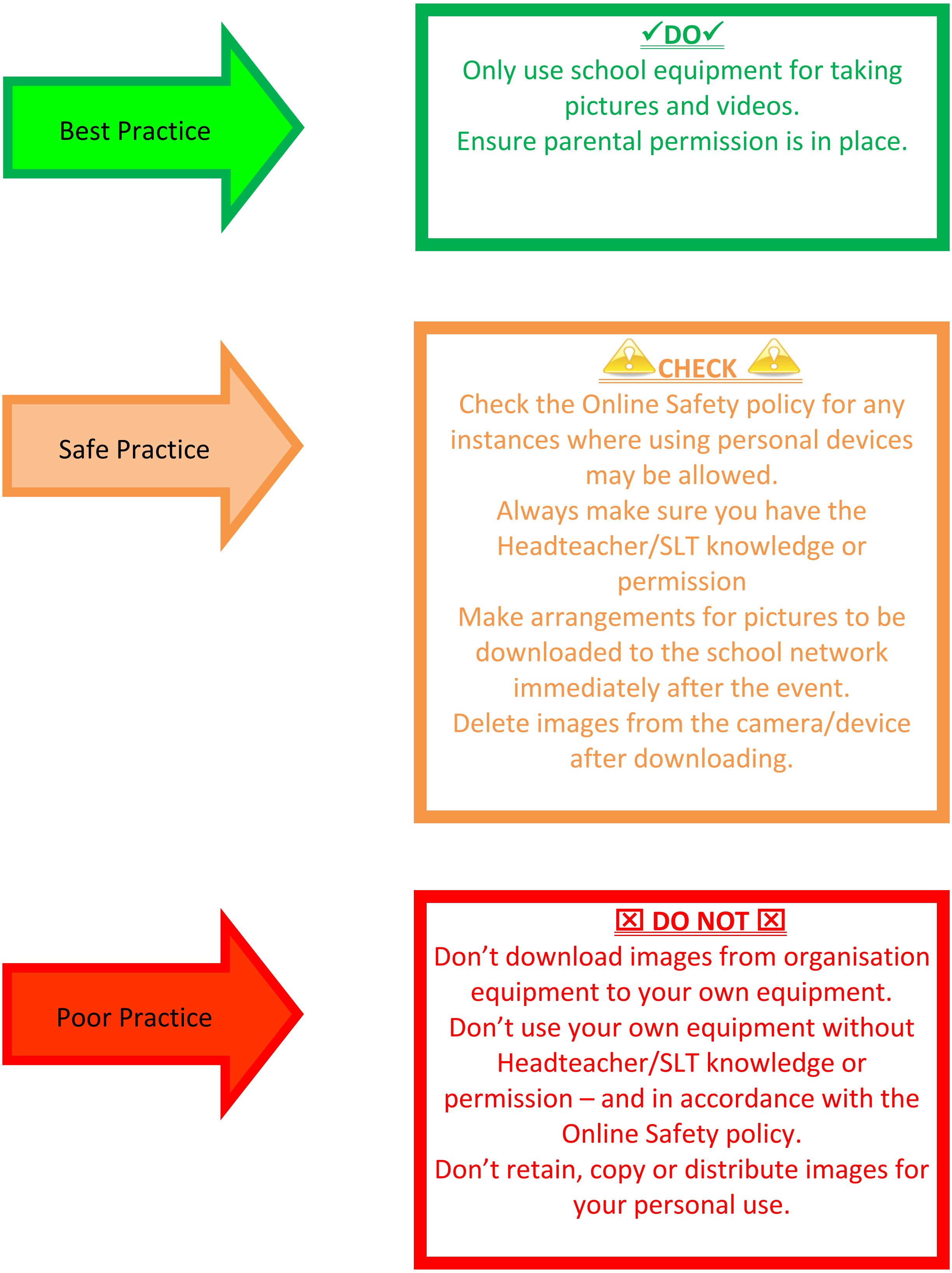
Poor Practice

☒ DO NOT ☒

Staff: don’t use your personal email account to communicate with students/pupils and their families in accordance with the Online Safety policy.

Good Practice Guidelines

Images, Photos and Videos



Best Practice

✓DO✓

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe Practice

⚠CHECK ⚠

Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor Practice

☒ DO NOT ☒

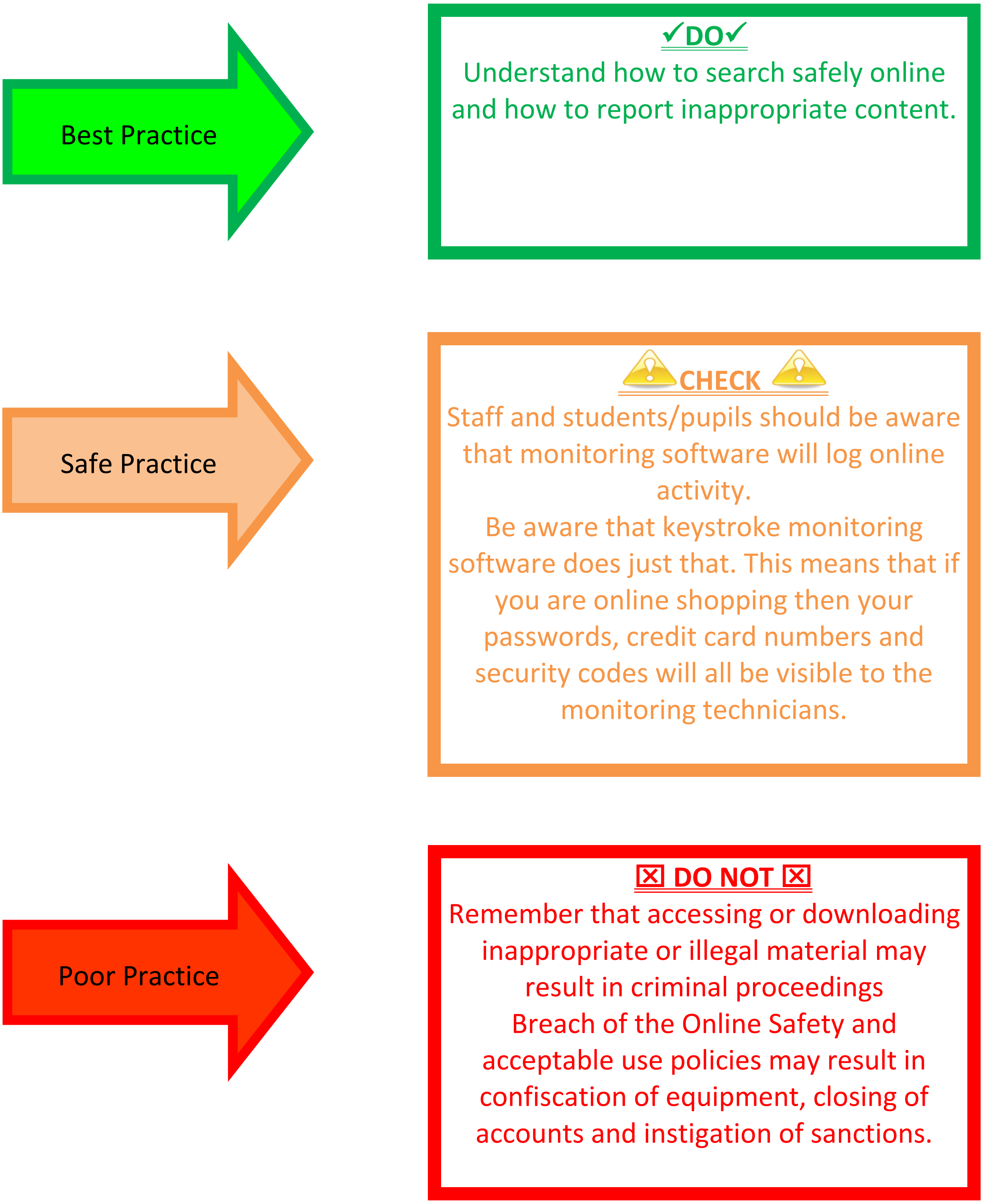
Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the Online Safety policy.

Don’t retain, copy or distribute images for your personal use.

Good Practice Guidelines

Internet



Best Practice

✓DO✓

Understand how to search safely online and how to report inappropriate content.

Safe Practice

⚠CHECK ⚠

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians.

Poor Practice

☒ DO NOT ☒

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the Online Safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Good Practice Guidelines

Mobile Phones

Best Practice

✓DO✓

Staff: If you need to use a mobile phone while on school business (trips etc), the school will provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe Practice

⚠CHECK ⚠

Check the Online Safety policy for any instances where using personal phones may be allowed.
Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor Practice

☒ DO NOT ☒

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.
Don't retain pupil/parent contact details for your personal use.

Good Practice Guidelines

Social Networking (e.g. Facebook / Twitter)

Best Practice

✓DO✓

If you have a personal account, regularly check all settings and make sure your security settings are not open access.
Ask family and friends to not post tagged images of you on their open access profiles.

Safe Practice

⚠ ⚠

Don’t accept people you don’t know as friends.
Be aware that belonging to a ‘group’ can allow access to your profile.

Poor Practice

☒ DO NOT ☒

Don’t have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don’t accept students/pupils or their parents as friends on your personal profile.
- Don’t accept ex-students/pupils users as friends.
- Don’t write inappropriate or indiscrete posts about colleagues, pupils or their parents.

Good Practice Guidelines

Webcams

Best Practice

✓DO✓

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe Practice

⚠CHECK⚠

Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor Practice

☒ DO NOT ☒

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the Online Safety policy.

Don’t retain, copy or distribute images for your personal use.

Incident Management

Should any of the following incidents occur the schools Online Safety Leader or Designated Safeguarding Lead (Front Door) should be informed **IMMEDIATELY**.

Inappropriate conduct will be investigated by the Headteacher following local authority protocols. Inappropriate conduct will be reported to the Local Authority Designated Officer for Safeguarding and police, where appropriate. Should the conduct be regarding the Headteacher, the Online Safety Leader must inform the Chair of Governors immediately.

Incident	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	DSL
Unauthorised use of non-educational sites during lessons	DSL
Unauthorised use of mobile phone/digital camera / other handheld device	DSL
Unauthorised use of social networking/ instant messaging/personal email	DSL
Unauthorised downloading or uploading of files	DSL
Allowing others to access school network by sharing username and passwords	Online Safety Lead
Attempting to access or accessing the school network, using another student's/pupil's account	Online Safety Lead
Attempting to access or accessing the school network, using the account of a member of staff	Online Safety Lead
Corrupting or destroying the data of other users	Online Safety Lead
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	DSL
Continued infringements of the above, following previous warnings or sanctions	DSL
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	DSL
Using proxy sites or other means to subvert the school's filtering system	Online Safety Lead
Accidentally accessing offensive or pornographic material and failing to report the incident	Online Safety Lead
Deliberately accessing or trying to access offensive or pornography	DSL
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	Online Safety Lead

Further information and support

- For a glossary of terms used in this document: http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf
- For Online Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People: http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf
- R u cyber safe?
  http://www.salford.gov.uk/rucybersafe.htm
  http://ico.org.uk/schools/primary-schools-lesson-plans
- Online Safety tips about how to stay safe online:
  http://www.salford.gov.uk/rucybersafe.htm
  http://www.thinkuknow.co.uk/
- Keeping Children Safe in Education September 2016

Clarendon Road Primary School

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Pupil: ***Class:***

Pupil's Agreement

I understand that I am responsible for my actions, both in and out of school:

- I will use the computer, network, mobile phones, internet and other new technologies in a responsible way at all times.
- I will not use the network and internet for anything which may be considered cyberbullying.
- I know that network and internet access may be monitored.
- I will be a responsible user and stay safe while using the internet and other technology for learning and personal use.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to consequences. This may include loss of Golden Time, loss of access to the school network/internet, exclusion, contact with parents and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website, blogs.

This agreement tries to ensure that ICT systems and users are protected from accidental or deliberate misuse. The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Signed: ***(Parent / Carer)*** ***Date:***

Clarendon Road Primary School's Online Safety Rules
Early Years & Key Stage One

Think then Click – to stay safe on the Internet.

- We only use the internet when an adult is with us.

- We can search the internet with an adult.

- We always ask if we get lost on the internet.

- We can click on a button or link when we know what they do or where they go.

→

- We never download anything from the internet without getting permission from an adult first.

- We never open emails from strangers. Tell your teacher if you get an email from a stranger.

- If you see something on the internet or in an email that makes you feel uncomfortable or unhappy, tell a teacher.

Clarendon Road Primary School's Online Safety Rules
Key Stage Two

✓I WILL✓	☒I WILL NOT☒
• Treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password • Immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online • Respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission • Be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions • Understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment • Immediately report any damage or faults involving equipment or software, however this may have happened	• Try (unless I have permission) to make downloads or uploads from the Internet • Take or share images (pictures and videos) of anyone without their permission • Use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission off a member of staff to do so. • Try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others • Try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials • Open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes • Attempt to install programmes of any type on a machine, or store programmes on a computer • Try to alter computer settings

Staff and Volunteer Acceptable Use Agreement

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- That staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For My Professional and Personal Safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, Virtual Learning Environment etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will only be possible to identify by first name, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my personal hand held/external devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's Online Safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Local Authority Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When using the internet in my professional capacity or for school sanctioned personal use:
  - I will ensure that I have permission to use the original work of others in my own work.
  - Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached. I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include investigation, warning, suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Position	
Signed	
Date	
Laptop (where relevant)	**Make:**
	Serial Number:
	Asset Tag:
	Machine Name: CLRP
	User Name:

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can only be identified by the use of their first names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

As the parent / carer of the above pupil, I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Parent / Carers Name	
Pupil Name	
Signed	
Date	