The De Montfort School

UNLOCKING YOUR CHILD'S POTENTIAL

E-Safety Policy

Agreed by Governing Body: 11.10.16.

Reviewed by Governing Body: 20.09.17.

E-Safety Policy for The De Montfort School

(based on Worcestershire Model Policy)

Review 12.9.18

Introduction

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended School and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

Several of the statements below can be directly related to aspects of e-safety:

Behaviour and safety of pupils at the school

When evaluating the behaviour and safety of pupils, inspectors consider:

- pupils' attitudes to learning and conduct in lessons and around the establishment
- pupils' behaviour towards, and respect for, other young people and adults, including freedom from bullying and harassment that may include cyber-bullying and prejudice-based bullying related to special educational need, sexual orientation, sex, race, religion and belief, gender reassignment or disability
- how well teachers manage the behaviour and expectations of pupils to ensure that all pupils have an equal and fair chance to thrive and learn in an atmosphere of respect and dignity
- pupils' ability to assess and manage risk appropriately and to keep themselves safe
- pupils' attendance and punctuality at school and in lessons
- how well the school ensures the systematic and consistent management of behaviour.

The Computing curriculum contains specific references to e-safety:

- **KS2**: use technology safely, respectfully and responsibly; know a range of ways to report concerns and inappropriate behaviour
- **KS3**: understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.
- **KS4**: understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to report concerns.

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children and young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that children and young people learn and are taught. At home, technology is changing the way children and young people live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.
- The potential to be drawn into terrorism through radicalisation via social media

This policy sets out how we strive to keep pupils safe with technology while they are in school. We recognise that children and young people are often more at risk when using technology at home (where often no controls over the technical structures are put in place to keep them safe) and so this policy also sets out how we educate them about the potential risks and try to embed appropriate behaviours. We also explain how we attempt to inform those people who work with our pupils beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our e-safeguarding policy has been written from a template provided by Worcestershire County Council which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of **all users** of ICT in our school.

It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

A.1.2 Responsibilities: e-safety coordinator

Our e-safety coordinator (Safeguarding Officer) is the person responsible to the head teacher and governors for issues relating to e-safety. The e-safety coordinator:

- takes responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of major e-safety incidents and monitors the log of incidents to inform future e-safety developments (*termly)*
- attends relevant meetings and committees of Governing Body

A.1.3 Responsibilities: governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. The Safeguarding Governor will liaise with the Safeguarding Officer over E-Safety issues.

A.1.4 Responsibilities: Head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though responsibility for e-safety is delegated to the Safeguarding Officer.
- The head teacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff.

A.1.5 Responsibilities: all staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of pupils and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**.
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices, including the school's approach to the Prevent Agenda.
- they are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified
- they have read, understood and signed the school's Acceptable Use Agreement for staff
- they report any suspected misuse or problem to the the Network Manager
- they undertake any digital communications with pupils (email / Virtual Learning Environment) in a fully professional manner and only using official systems
- they embed e-safety issues in the curriculum and other activities, also acknowledging the planned e-safety programme

A.1.6 Responsibilities: System Network Manager

Is responsible for ensuring that:

- the schools ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance)
- users may only access the school networks through a properly enforced password protection policy as outlined in the school e-security policy
- shortcomings in the infrastructure are reported to the Network Manager so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

This e-safety policy has been developed (from a template provided by Worcestershire County Council) by a working group made up of:

- *Safeguarding officer Deputy Headteacher*
- *Network System Manager*

And there has been consultation with Senior leaders, Safeguarding Governor and pupils.

This e-safety policy was approved by the governing body on:	
The implementation of this e-safety policy will be monitored by the:	*Network Systems Manager and Deputy Head in charge of Safeguarding*
Monitoring of this policy will take place at regular intervals:	*Bi-annually*

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Local Authority Designated Officer* *Worcestershire Senior Adviser for Safeguarding Children in Education* *West Mercia Police*

A.2.2 Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, radicalisation or other e-safety incidents covered by this policy, which may take place out of the school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

A.2.3 Acceptable Use Agreements

All members of the school community including technicians, whether directly employed or from external technical support teams, are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils
- Staff (and volunteers)
- Technical support personnel

Restricted use is given on occasion to

- Parents / carers
- Community users of the school ICT system

Acceptable Use Agreements are introduced in Year 6 in ICT lessons and agreed to by all pupils as they enter school. This agreement is made annually on the school system for all students and staff.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school ICT system.

Induction system for all members of the school community include this guidance and the AUP

A.2.4 Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies and other policies or procedures relating to e-safety

School systems and Data Security Policy	How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the e-safety policy.
Anti-bullying	How your school strives to eliminate bullying – link to cyber bullying

Safeguarding	Safeguarding pupils electronically is an important aspect of E-Safety. ***The e-safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging all aspects of safety and sanctions for disregarding it.
Use of images	**WCC guidance to support the safe and appropriate use of images in schools, academies and settings**

A.2.5 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in an education context and that users should not engage in these activities when using school equipment or systems (**in or out of school**).

Users shall not visit Internet sites, make, post, download, upload, transfer data, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images (illegal - The Protection of Children Act 1978)
- grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- criminally racist material in UK – to stir up religious hatred including radicalisation as per the Prevent Agenda (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- pornography
- promotion of any kind of discrimination including 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

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- *Using school systems to undertake transactions pertaining to a private business*
- *Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband and or the school system*
- *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 gambling and non-educational gaming*
- *On-line shopping / commerce unless directly related to school business*
- *Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)*

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a **proportionate** manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse. In serious cases the Headteacher and Safeguarding Officer will be informed in order to take appropriate action.

A.3.1 Use of hand held technology (personal phones and other hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- ✓ *Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:*
  - ✓ *Personal hand held devices will be used in lesson time only in an educational capacity or emergency*
  - ✓ *Members of staff are free to use these devices outside teaching time.*
  - ✓ *A school mobile phone is available (for example when engaging in off-site activities) to provide a number to students or parents.*
- ✓ *Pupils are restricted at High School to having phone access at break times only, at other times phones should be switched off and out or site. At Middle School phones should be kept in lockers. Some use may be made of phones in lessons when considered appropriate by a teacher. If linked to the school network system users will sign an additional agreement, use will be restricted and monitored.*

	Staff / adults				Pupils			
Personal hand held technology *This table has been reviewed in the light of principles agreed within TDMS.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought into the school	✔					✔		
Use of mobile phones in lessons		✔				✔		
Use of mobile phones in social time		✔				✔		
Taking photos on personal phones or other camera devices		✔				✔		
Use of hand held devices e.g. PDAs, gaming consoles	✔					✔		

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all pupils.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others regarding school business when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- Pupils normally use their email account to communicate with people outside school with the permission / guidance of their teacher
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)

- Users must immediately report to their teacher– in accordance with this policy (see sections A.2.6 and A.2.7) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

The exception for this is the school Twitter and Facebook accounts.

	Staff / adults				Pupils			
Use of social networking tools *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non-educational chat rooms etc				✔				✔
Use of non-educational instant messaging				✔				✔
Use of non-educational social networking sites		✔ *						✔
Use of non-educational blogs				✔				✔

*Use of TDMS Twitter by staff

TDMS values the use of specific social media to support the education of students, as well as wider curricular use and in communication with parents and the wider community.

- Staff and pupils should use only the social networking services to communicate with others regarding school business when in school, or on school systems (e.g. by remote access)
- Users need to be aware that communications may be monitored
- Students will use social media to communicate with people outside school only with the permission / guidance of their teacher
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of social media (see section C of this policy)
- Staff may only access personal social networking sites on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)
- Users must immediately report to their teacher– in accordance with this policy - the receipt of any message that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such message.

A.3.2c - Videoconferencing

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.

External IP addresses should not be made available to other sites.

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the teacher before making or answering a videoconference call.

Permission for pupils to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in the school. Only where permission is granted may pupils participate.

Only key administrators have access to videoconferencing administration areas. They will check permission has been granted from parents/carers.

A.3.3 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they

should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images. Those images should be captured using school equipment if the personal equipment of staff is used pictures should be downloaded (or uploaded onto Twitter) immediately and deleted from the device.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph (e.g. some looked after children)
- Pupils must not take, use, share, publish or distribute images of others without their permission

A.3.4 Use of web-based publication tools

A.3.4a - Website (and other public facing communications)

Our school uses the public facing website only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of pupils. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website, and only then when necessary.
- Detailed calendars will not be published on the school website.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
  - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
  - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

A.3.4b – Learning Platform

The use of the learning platform by pupils is monitored.
User accounts and access rights can only be created by the VLE administrator
Pupils are advised on acceptable conduct and use when using the learning platform.
Only members of the current pupil, parent/carers and staff community will have access to the learning platform.
When staff, pupils, etc. leave the school their account or rights to specific areas will be disabled.
Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the learning platform may be suspended for the user.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A pupil's parent/carer may be informed.

A.3.5 Professional standards for staff communication

In all aspects of their work in our establishment, teachers abide by the broad Professional Standards for Teachers. Staff also adhere to the LA Guidance for Employees which includes a Code of Conduct as well as the staff Acceptable User Policy.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform, etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

The school e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy). Staff password must remain secure and not shared with students. Staff users will be required to change passwords each half term as standard practice.

B.2.1 Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering system to manage the associated risks and to provide preventative measures which are relevant to this school.

As a school buying broadband services procured by Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

B.2.1a - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **Network Manager** (with ultimate responsibility resting with the **head teacher and governors**). They manage filtering and keep logs of breaches of the filtering system.

All users have a responsibility to report immediately to teachers / network manager any infringements of the filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1b - Education / training / awareness

Pupils are made aware of the importance of filtering systems.
Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed through website information.

B.2.1c - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school Network Manager.
- He checks the website content to ensure that it is appropriate for use in school.
- If agreement is reached, the e-safety coordinator makes a request to IBS Schools Broadband Team, or other filtering provider

The Network Manager will need to apply a rigorous system for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

B.2.1d - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the network and on school equipment.

Monitoring takes place as follows:

- At least 2 identified members of staff review the monitoring console captures in turn, weekly.
- Potential issues are referred to an appropriate person depending on the nature of the capture. Serious incidents are reported to the Safeguarding Officer as well as Behaviour Support Team.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

Filter change-control logs and incident logs are made available to Safeguarding Officer and WSCB if requested. This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

B.2.2 Technical security

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document referred to in the introduction for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document referred to in the introduction for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school. (see section C of this policy)

Section C. Education

C.1.1 E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need constant help and support to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping them to learn how to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of Computing lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and beyond school.
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the pupil Acceptable Use Agreement (see Appendix 1) and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

C.1.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing appropriate techniques.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/. These are mediated by a CEOP trained teacher.

C.2 Staff training

It is essential that all staff – including non-teaching staff - receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-Safety training will be available and updated.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements, which are signed as part of their induction
- Computing teachers and the Safeguarding Officer will be CEOP trained and keep up to date with guidance documents.
- The Safeguarding Officer/Network Manager will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from appropriately qualified persons when required.

C.3 Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or child protection.

C.4 Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through e.g. Parents Information Evening, the school website, emails, leaflets and text links/advice.

Appendix 1d - Acceptable Use Agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- young people will be responsible users and stay safe while using ICT (especially the internet).
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of their work.

Child's name	
Parent's name and signature	
Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at the school/

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe and responsible use of ICT – both in and out of the school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use the school's digital cameras to record evidence of activities in lessons and out of the 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. The school will also ensure that when images are published, the young people cannot be identified by name.

As the parent/carer of the above pupil, I agree to the school taking and using digital images of my child(ren). 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 school events which include images of children, I will abide by these guidelines in my use of these images. I agree that I will not post such images of children, other than my own, on social networking sites.

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the website *and in the learning platform.*

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Permission to for my child to participate in video-conferencing

Videoconferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas educational partner. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

The school's e-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

A sample document for recording the review of and action arriving from the review of potentially harmful websites can be found on the next page

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Appendix 3 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

B. CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- **The site promotes equal and just representations of racial, gender, and religious issues.**
- **The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.**
- **The site does not link to other sites which may be harmful / unsuitable for the pupils**
- The content of the website is current.

C. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 4 - Supporting resources and links

The following links may help those who are developing or reviewing a school e-safety policy.

General

South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe

Child Exploitation and Online Protection Centre (CEOP) http://ceop.police.uk/

ThinkUKnow http://www.thinkuknow.co.uk/

ChildNet http://www.childnet.com/

InSafe http://www.saferinternet.org/

Byron Reviews ("Safer Children in a Digital World") - https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Becta – various useful resources now archived
http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk

London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Northern Grid - http://www.digitallyconfident.org

National Education Network - http://www.nen.gov.uk/e-safety/

WMNet – http://www.wmnet.org.uk

EU kids Online - http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx

Cyber Bullying

Teachernet "Safe to Learn – embedding anti-bullying work in schools" (Archived resources)

http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/academy/behaviour/tacklingbullying/cyberbullying/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Prevent Duty -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Social networking

Digizen – "Young People and Social Networking Services": http://www.digizen.org/socialnetworking/

Get Safe On-line - https://www.getsafeonline.org/social-networking

Connect Safely - Smart socialising: http://www.connectsafely.org/

Mobile technologies

"How mobile phones help learning in secondary schools":

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

"Guidelines on misuse of camera and video phones in school/academies"
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

Digital Parenting - http://www.vodaphone.com/parents

http://www.digitalparenting.ie/

https://www.commonsensemedia.org/

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Internet Watch Foundation: http://www.iwf.org.uk

Digizen – cyber-bullying films: http://old.digizen.org/cyberbullying/film.aspx

Appendix 6 Template Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 7 Guidance to support the safe and appropriate use of images in schools and settings

Based on:

Safeguarding Children and Safer Recruitment in Education – *Consultation version 2010*

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings – *DCSF March 2009*

Data Protection Good Practice Note: Taking Photographs in School – *Information Commissioner's Office 26th October 2007*

Contacts:

Sally Mills, Senior Advisor, Safeguarding Children in Education SMills@worcestershire.gov.uk

Cath Ellicott, Early Years and Childcare Manager

CEllicott@worcestershire.gov.uk,

Introduction

There are many occasions when staff and parents will want to take photographs of children. Such occasions include everything from observation, evidence, assessment and curricular purposes in the classroom to award ceremonies, performances, trips and sporting events as part of the extended activities programme. The intention of this policy is to set out clear guidelines which will balance the use of photography as a source of pleasure and pride with the need to safeguard children and protect the rights of the individual.

The photography policy sets out to ensure that:

- Photographs are only used for the purpose intended
- Settings use of photographs is facilitated
- Personal family photography is allowed where possible
- Individual rights are respected and child protection issues considered
- Parents/carers and children are given the right to opt out.

Definitions

The term 'images' refers to photographic prints or slides, digital images, videos or moving images. Images may be distributed via print, DVDs, the internet or other technologies.

Safeguarding Children

The welfare and protection of our children is paramount and consideration should always be given to whether the use of photography will place our children at risk. Images may be used to harm children, for example as a preliminary to 'grooming' or by displaying them inappropriately on the internet, particularly social networking sites.

For this reason consent is always sought when photographing children and additional consideration given to photographing vulnerable children, particularly Looked After Children or those in domestic abuse situations. Consent must be sought from those with parental responsibility (this may include the Local Authority in the case of Looked After Children).

Data Protection

The Information Commissioner's Office (ICO) maintains a public register which includes the name and address of 'data controllers' and details about the types of personal information they process. 'Notification' is the process by which each data controller's details are added to the register. All settings need to ensure they are registered with the Information Commissioner's Office every year. Failure to notify the ICO is a criminal offence. Notification is

necessary if settings are processing personal information. This includes taking photographs of the children using a digital camera. Personal data (including photos) held by settings must be included in the setting's notification. Further information on data protection as well as details on how to notify can be found at:http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

In October 2007, the Information Commissioner's Office issued the following advice:

"The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- *Photos taken for official school use may be covered by the act and pupils and students should be advised why they are being taken.*
- *Photos taken purely for personal use are exempt from the Act."*

Please note that although notification is mandatory in most cases the data protection guidance within this document is 'recommended guidance' and settings must take individual responsibility for their own data protection issues in accordance with the Data Protection Act 1998.

Parental Consent

On admission of a child to a setting, parents/carers will be asked to complete a consent form indicating their agreement or objection regarding the use of images of their child. Consent should be discussed with the child, once they are old enough to understand, and the child also asked to sign the consent form. Parents/children should be asked to complete the separate WCC consent form for images that have been taken for the purpose of LA publicity.

A list of children for whom consent has been refused will be maintained by the setting and every effort will be made by staff not to include these children in photographs or video footage. The list will be updated on a regular basis[1].

The parent/carer should be asked to confirm, in writing, that they will inform the setting if they no longer wish images of their child to be used for any reason. They need to be made aware that once images are in circulation or have been published, it may be impossible to remove them, although every effort will be made to ensure they are not used in future publications.

Setting Photography

Photographic and/or video images taken by staff may be used for curricular and/or extra-curricular activities, displays, on the setting website, in the setting prospectus or newsletter, as evidence of the child's development or as part of publicity in the media. Staff will ensure that:

- They are clear about the purpose of the activity and what will happen to the images when the activity is concluded.
- Any images taken using their personal camera, mobile phone or video equipment or for their own personal use are deleted as soon as they are uploaded.
- They will never photograph children in a state of undress, for example whilst changing for PE or a performance.
- They will report any concerns about inappropriate or intrusive photographs found to the Senior Designated Person following the setting's safeguarding procedures
- They have parental permission to take; store and/or display the images.

Storage of Images

Photographs retained in a setting will not be used other than for their original purpose, unless permission is obtained from the subject.

Images should always be stored securely and password protected.

---

[1] The LA recommends on admission to a setting with at least annual updates

Photographs should be destroyed or deleted from databases once they are no longer required for the purpose for which they were taken. Photographs taken for publicity and promotional purposes should be retained for a maximum of two years. Photographs contributing to the history of the setting, its children, activities or the community, may be retained indefinitely.

For schools, further information on storage and security can be found in the LA guidance *Schools System and Data Security.*

Parental Photography

In many cases, photographs taken at setting events form an important part of family albums. Everything possible will be done to ensure that this tradition continues. Parents are welcome to take photographs of their own children at award ceremonies, setting concerts/shows and sporting events, with the permission of the Headteacher. However, care must be taken not to interfere with the smooth running of the event, breach commercial copyright laws or compromise health and safety. Parents/carers will ensure that:

- They will respect the setting's decision to prohibit photography of certain children or a particular event.
- Any images taken are for personal use only.
- Images including children **other than their own, must not be sold or put on the internet**; if they are, Data Protection legislation may be contravened and they will be asked to remove them.
- They will not use any images of children so as to cause offence or harm.

The Use of Cameras and Video Recordings by Children

From time to time, children may be given the opportunity to use setting equipment to take photographs and/or video footage as part of a curricular or extra-curricular activity.

Children should not use personal equipment in the setting for the purpose of taking photographs or video footage, unless being used as a learning resource in line with the setting's Acceptable Use policy. This includes the use of personal Smartphones. The only exception to this is on a setting trip or visit where children may be allowed to take photographs for their own personal use.

It should be made clear that these images should be taken responsibly and not used to upset any other child

The use of images to bully or intimidate, including publishing photographs without permission on the internet, will be dealt with in line with the setting's behaviour and anti-bullying policies and may be viewed as a criminal offence.

Display of photographs

It is perfectly acceptable to display photographs of children in the setting environment with their names attached for the purpose of celebrating progress and achievement or assessment purposes.

However, all settings must give consideration to displays when rooms are available for other purposes.

Publicity

Press

On occasions, the media are asked to cover setting events or to highlight children's successes. This is an important part of celebrating achievement and informing the public of educational initiatives. The media operate under their own Code of Practice. Parents will be informed by the setting in advance if their children are likely to appear in the press. Local newspaper titles may share their images with other titles within the same syndicate. Any child whose parents have withheld permission, will not be photographed by the media.

Setting Publicity

Photographs of children's activities and achievements may be published in the setting newsletter or prospectus and posted on the setting website. Names of individual children will not be attached to photographs and no contact details will be published. Where photographic permission has been withheld, photographs will not be published.

Setting Photographer

Class and individual or group photographs are often an annual event. Parents will be notified in advance of the photographer's visit and will be sent copies of photographs and given the option to purchase them. Copyright on all such photographs is retained by the photographer.

Links

This guidance should link specifically to the setting's Data Security Policy, E-safety Policy, Acceptable Use Policy, Password Policy, Staff Laptop Policy, Safeguarding Children Policy and to the LA guidance 'Schools System and Data Security'.

Further Guidance

Further related guidance can be found in the Becta series of documents entitled *Good practice in information handling in schools*. They are:

1 Keeping data secure, safe and legal
2 Impact levels and labelling
3 Audit logging and incident handling
4 Data encryption
5 Secure remote access
and also in *AUPs in context: Establishing safe and responsible online behaviours*
These documents can be found on Edulink (www.edulink.networcs.net) and on the Department for Education website (www.education.gov.uk).

Consent Form for use of Images (photographs, videos, DVDs and digital images)

Photographs and/or video recordings of children may be taken whilst they attend the setting to celebrate their achievements and successes and as evidence of their progress and development. Still or moving images may be published in our printed publications (e.g. prospectus, newsletters) and/or on our external websites. They may also be used to promote the good practice of the setting to other teachers, e.g. at training events organised by the Local Authority or national education/government institutions. Children's names will never be published alongside their photograph externally to the education setting. Names may be used internally, for example – on a display.

Electronic images, whether photographs or videos, will be stored securely on the setting's network which is accessible only by authorised users.

Before using any photographs/videos of your child we need your permission. **Please answer the questions below, then sign and date the form where indicated and return it.**

Please circle

1. May we use your child's photograph in printed publications? **Yes / No**

2. May we use your child's photograph on our internet websites? **Yes/No**
3. May we allow your child's photograph (e.g. as part of a team or record of an event) to be used for publication in a newspaper? **Yes / No**
   (Please note that the use of photographs in newspapers is subject to strict guidelines)

4. May we use any photograph or video of your child internally as part of regular activities and work of the setting? **Yes / No**

5. May we use any photographs or video containing your child to share good practice with staff from other settings? **Yes / No**

6. May we use images of your child on an external web site or for publicity or campaigns by national Government agencies? **Yes/No**

This form is valid from the date of signing until your child leaves the setting. Photographs and videos may be securely archived after your child has left the setting. Photographs and videos used for publicity purposes may continue to remain in circulation after your child has left the setting. You may withdraw your consent, in writing, at any time **but it may not be possible to remove images that are already in circulation or have already been published** although every effort will be made to do so.

We recognise that parents, carers and family members will wish to record events such as plays, sports days etc. to celebrate their child's achievements. The setting is happy to allow this, at the discretion of the Headteacher/Senior Manager, on the understanding that such images/recordings are used for purely personal family use. Images containing children **other than their own** should not be put on the internet for any reason, without first seeking permission from the other child's parents/carers.

A full copy of the setting's policy on the safe use of children's photographs may be obtained upon request.

Name of Child: …… Date of birth: ……

Signed: …… Date: ……

(if appropriate)

Name of person with Parental Responsibility: ……

Signed: …… Date: ……

Data Protection

The De Montfort School takes your privacy seriously and we have taken steps to protect it. Any personal data you give to us, including photographic images, will be processed strictly in accordance with the Data Protection Act 1998 and will be used for the purposes that you have consented to. We will not share your details with third parties without your consent, except where we are legally compelled or obligated to do so. Please note that where you consent to images appearing on the internet, they can be viewed worldwide including countries where UK data protection law does not apply.

Appendix 8 Social Networking Staff Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.

- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.

- Do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.

- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.

- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.

- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.

- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

Name		***Date***	
Print Name			

The De Montfort School

Appendix 9 Loaned Device User Agreement

Staff member: Date:

Device Make: Model : Serial Number :

The laptop/device detailed above is loaned to Xxxxxxxxxxx Xxxxxxxxxx for the duration of their employment at Xxxxxxxxxxxxx Xxxxxx School subject to the following terms and the school Acceptable Use Agreement.

The iPad/mobile device remains the property of the School and must be returned at the end of the contracted period of employment with the School and, if required, during a planned or prolonged absence.

1. The laptop/device is for the **work related** use of the named member of staff to which it is issued.

2. Only software/apps installed at the time of issue or software/apps purchased by and licensed to Xxxxxxxxxxxxx Xxxxxxx School may be installed on the machine.

3. The laptop/device remains the property of the School throughout the loan period, however the member of staff to which it is issued **will** be required to take responsibility for its care and safe keeping.

4. If left unattended the laptop/device must be securely stored. It must **never** be left unattended even for a short period in a car, including in a locked boot.

5. Due regard must be given to the security of the computer if using other forms of transport.

6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality, under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data, including images.

7. The equipment must be docked in the school charging and syncing cabinet at least once per week to ensure updates and new software are distributed. Staff should record this action in the log provided with the syncing cabinet.

8. The laptop/device will be recalled from time to time for routine maintenance / upgrade and monitoring.

Prohibited Uses

Images of other people, including children, may only be made with the permission of the person, or parents of the child, in the photograph.

The laptop/device is a professional tool designed to enhance classroom practice. It is not for personal use, e.g. Facebook or other social networking sites or on-line shopping, and should remain in school unless permission is sought from the ICT Co-ordinator or Head Teacher.

Lost, Damaged or Stolen laptop/device

If the laptop/device is lost, stolen or damaged, the Network Manager or Head Teacher must be informed immediately and a charge may be levied depending on the circumstances.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the laptop or device and return it immediately upon request.

Signed: _____

Date: _____