High View Primary Learning Centre eSecurity and eSafety

Introduction

We must demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce the risks posed by the digital technologies used in teaching and learning in our school. The eSafeguarding policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

Please note that this policy also adheres to (and is enhanced by) the ECM Academy Trust Information Security and ICT Usage Policy.

Scope of the Policy

- This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
- 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 the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other eSafeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others
- The school will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents / carers of incidents of inappropriate eSafeguarding behaviour that take place out of school.

Development, Monitoring and Review of this Policy

This policy has been developed by a working group / committee made up of the following people:

- School ESafety Co-ordinator – Lois Mundy
- ICT Technical Support – Mick Haworth
- Head of School – Theresa Smith
- ECM Trust Business Manager – Tim Marsh

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council and Class Council
- Governors meeting / subcommittee meeting

Because of the regular updates of the policy there may be many versions created, each version will be stored for audit purposes.

Title	ESafeguarding Policy
Version	1.0

Date	16/3/2017
Author	L.Mundy
This eSafeguarding policy was approved by the Governing Body on:	
Monitoring will take place at regular intervals (at least annually):	Annually
The Governing Body will receive a report on the implementation of the policy including anonymous details of any eSafeguarding incidents at regular intervals:	Annually
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to eSafety or incidents that have taken place. The next anticipated review date will be:	January 2018
Should serious eSafeguarding incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office, CEOP.

- The school will monitor the impact of the policy using:
- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

All staff and members of the school community will be informed of any relevant amendments to the policy.

Communication of the Policy

- High View's senior leadership team, along with the eSafety co-ordinator, will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy that applies to them and the use of any new technology within school.
- The eSafeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all affected members of the school community.
- Any relevant amendments will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.

- An eSafeguarding or eSafety module will be included in the PSHE, Citizenship and/or ICT curricula, covering and detailing amendments to the eSafeguarding policy, particularly focussing on the Acceptable Use Policy, in order to introduce it to all of the pupils in school.
- An eSafeguarding or eSafety training programme will be established across the school to include a regular review of the eSafeguarding policy.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used.

Roles and Responsibilities

We believe that eSafeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team:

- The Executive Head has overall responsibility for eSafeguarding all members of the school community, though the day to day responsibility for eSafeguarding will be delegated to the ESafeguarding Co-ordinator.
- The Executive Head and senior leadership team are responsible for ensuring that the eSafeguarding Co-ordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The Executive Head and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal eSafeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the eSafeguarding Coordinator.
- The Executive Head and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident (see flow chart on dealing with eSafety incidents included in a later section and relevant Local Authority HR / disciplinary procedures).
- The Executive Head and senior leadership team should receive update reports on eSafeguarding incidents from the eSafeguarding Co-ordinator.

Responsibilities of the eSafeguarding Committee

- To ensure that the school eSafeguarding policy is current and pertinent.
- To ensure that the school eSafeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

Responsibilities of the eSafeguarding Co-ordinator

- To promote an awareness and commitment to eSafeguarding throughout the school.
- To be the first point of contact in school on all eSafeguarding matters.
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures. ▪ To lead the school eSafeguarding group or committee.
- To have contact with other eSafeguarding committees whenever necessary, e.g.

Safeguarding Children Board, in order to keep up to date with current issues and to address more serious incidents that may arise.

- To communicate regularly with school technical staff.
- To communicate regularly with the designated eSafeguarding governor.
- To communicate regularly with the senior leadership team.
- To create and maintain eSafeguarding policies and procedures.
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- To ensure that eSafeguarding education is embedded across the curriculum.
- To ensure that eSafeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on eSafeguarding issues to the eSafeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- To ensure that an eSafeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To read and understand the pupils' Acceptable Use Policy and to ensure that it is adhered to by pupil.
- To report any suspected misuse or problem to the eSafeguarding Co-ordinator.
- To develop and maintain an awareness of current eSafeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology (both inside and outside school).
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times – this includes never being friends with pupils on social media sites etc and only being friends with parents of pupils if they are your personal friends. In addition, you should be aware that, when posting anything on social media sides, you should behave in the same professional manner that you would do in school. Would you be happy for your pupils / parents of your pupils seeing your posts?
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.

- To report any eSafeguarding related issues that come to your attention to the eSafeguarding Co-ordinator.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices and that such data and information is encrypted.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, work placement students and volunteers
This section covers an area of professional concern that has become more relevant in recent years. The appendix to this document includes references to some important guidance – in particular the "Guidance for Safer Working Practice for Adults who work with Children and Young People"

Communication between adults, and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs. Below is an outline of rules and guidance. For further detail, see the ECM Academy Trust Social Media Policy.

When using digital communications, staff and volunteers should:
- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person on social networks.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children so as to avoid any possible misinterpretation.
- ensure that, if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the school into disrepute.

- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Child Protection Officer

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyber bullying and the use of social media for this purpose.

Responsibilities of Pupils

Below is an outline of rules and guidance. For further detail, see the ECM Academy Trust Social Media Policy.

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies on the taking and use of mobile phones in school.
- To know and understand school policies regarding cyber bullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies, both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss eSafeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

Below is an outline of rules and guidance. For further detail, see the ECM Academy Trust Social Media Policy.

- To help and support the school in promoting eSafeguarding.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.
- To sign a home-school agreement containing the following statements:

- ✓ We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.
- ✓ We will support the school's stance on the use of ICT and ICT equipment.

- Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet.
- Parents may take photographs at school events. However, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school (see appendix).
- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances (see appendix).

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the eSafeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.

The role of the ESafety Governor includes the following:

- regular meetings with the ESafety Co-ordinator
- regular monitoring of eSafety incident logs
- reporting to Governors meeting

Responsibilities of Other Community / External Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

- The school will liaise with local organisations to establish a common approach to eSafeguarding and the safe use of technologies.
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate.
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school and that the account that they use to log on to the school ICT system will give them limited access and no access to personal files, data etc.

Education

Pupils

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 eSafety is therefore

an essential part of the school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience.

eSafety education will be provided in the following ways:

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the PSHE curriculum, as well as eSafeguarding specific lessons when necessary within a specific class in order to address any issues that have arisen.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy, which will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies (i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button).

All Staff (including Governors)

It is essential that all staff receive eSafety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Relevant eSafety training will be made available to staff.
- An audit of the eSafety training needs of all staff will be carried out regularly.
- All new staff will receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies.
- This eSafeguarding policy and its updates will be presented to and discussed by staff in staff / team meetings.
- The eSafety Co-ordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through

- parents' evenings
- newsletters
- letters

- leaflets
- website
- information about national / local eSafety campaigns / literature

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (eg on social networking sites).
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. If personal equipment is used, photographs must be deleted from it before it leaves the school premises.
- 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published publicly on the website, or elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, and no names will be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Where photographs are published publicly online, they will not be associated with children's names.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive. At Key Stage 2, from September 2016, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

Filtering Internet Access

- The school uses a filtered internet service. The filtering system is provided by Lightspeed Rocket.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Co-ordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Co-ordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP (Child Exploitation and Online Protection Centre) or the IWF (Internet Watch Foundation).
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Key Stage 2 will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Staff users will be prompted to change their passwords at prearranged intervals (every 3 months) or at any time that they feel their password may have been compromised.
- Staff should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords.
- System passwords will not be written down.
- Staff will only disclose their personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Users will always use their own personal passwords to access computer based services, never share these with other users.
- Staff will make sure they enter their personal passwords each time you logon. Do not include passwords in any automated logon procedures.

- Staff will never save system-based usernames and passwords (ie school email) within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and, where possible, special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Data Protection

Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights • Secure
- Only transferred to others with adequate protection.

Based on this, we have made the following decisions about the handling of data at High View PLC:

- At all times, we take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- We use personal data only on secure password protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data or their computer is locked when left unattended.
- Certain members of staff have all data on their portable devices encrypted, where it is necessary that they have personal data saved on the said device.
- We transfer data using encryption and secure password protected devices.
- NO personal data is stored on portable devices that are taken off site. It should be stored on the school's network server and only accessed on site or via the VPN.

- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school is controlled appropriately through technical and non-technical access controls.
- Users are vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO.
- All information on school servers is accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO.
- Staff and pupils must not leave personal and sensitive printed documents on printers within public areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured, using 7-Zip where appropriate.

All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

If you are transmitting sensitive information or personal data e.g. by email or fax it must be transferred by a secure method so it is protected from unauthorised access (7-Zip)

Email

- Staff will never use public or personal email accounts for sending and receiving sensitive or personal data.
- Staff will not include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.
- Encryption makes a file non readable to anyone who does not have the password to open it. Therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

FAX

- Fax machines will be situated within controlled areas of the school.
- All sensitive information or personal data sent by email or fax will be transferred using a secure method.

Communication Technologies

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	*						Y6 only with parental agreement signed.	
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones				*				*
Taking photos on personal cameras		* Must be deleted from device before it leaves school premises. Permission must be granted from SLT.						*
Use of hand held devices eg PDAs, PSPs	*					*		
Use of personal email addresses in school, or on school network	*							*
Use of school email for personal emails				*				*

Use of chat rooms / facilities		*Not during lessons.						*
Use of instant messaging		*Not during lessons.						*
Use of social networking sites		*Not during lessons.						*
Use of blogs	*					*		

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

ceptable	Acceptable at certain times	Acceptable for certain users	ɐptable	ɔtable ıal

User Actions	Unsuitable / Inappropriate Activities	Ac				
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, eg 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				✓	
	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 SWGfL 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 (eg 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)			✓ Not in lessons			
On-line gambling			✓ Not in lessons			
On-line shopping / commerce			✓ Not in lessons			

File sharing		✓ Of legal files that do not include personal data.			
Use of social networking sites		✓ Not in lessons			
Use of video broadcasting eg Youtube	✓ Appropriate content only				

Responding to incidents of misuse
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 or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SSCB flow chart will be consulted and actions followed in line with the flow chart.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

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 as follows:

Pupils Actions / Sanctions

Please note that actions / sanctions are on a sliding scale, depending on the seriousness on the content and whether it is a first or repeat offence. Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓		✓	✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓				✓			✓ No longer allowed phone in school
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓		✓	✓	
Unauthorised downloading or uploading of files	✓	✓	✓		✓	✓	✓	✓	
Allowing others to access school network by sharing username and passwords	✓	✓			✓		✓		
Attempting to access or accessing the school network, using another student's / pupil's account	✓	✓			✓	✓	✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓		✓	✓	✓		✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		✓	✓			✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓		✓

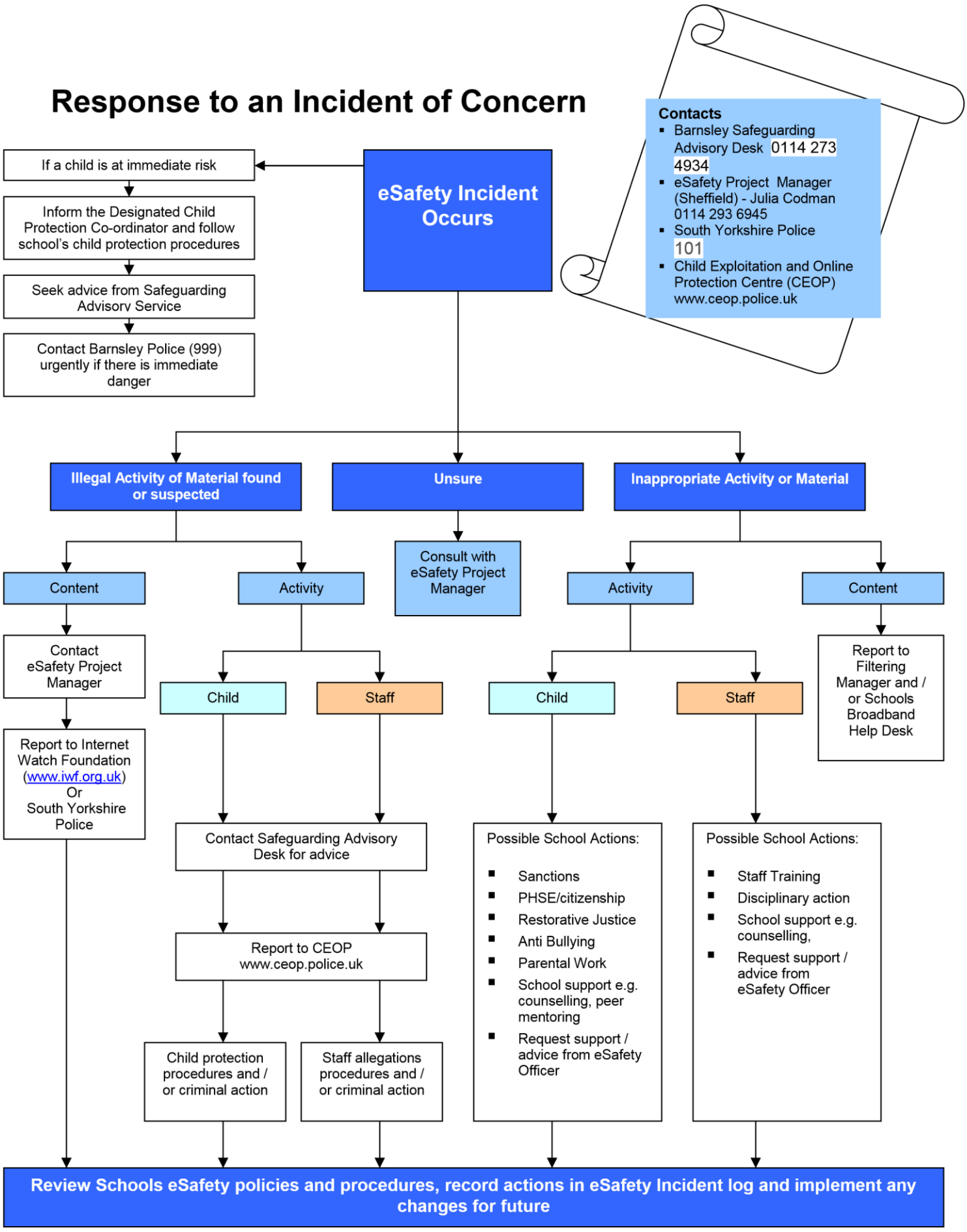
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓			✓	

Staff Actions / Sanctions

Please note that actions / sanctions are on a sliding scale, depending on the seriousness on the content and whether it is a first or repeat offence. Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓		✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓			✓	✓		✓
Unauthorised downloading or uploading of files		✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓			✓	✓		✓
Careless use of personal data eg holding or transferring data in an insecure manner		✓			✓	✓		✓
Deliberate actions to breach data protection or network security rules		✓			✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓	✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓	✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓			✓	✓		✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with parents in an unprofessional manner and bringing the school into disrepute		✓			✓	✓		✓
Actions which could compromise the staff member's professional standing		✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓				✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓		

Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓		✓
Deliberately accessing or trying to access offensive or pornographic material		✓			✓		✓	✓
Breaching copyright or licensing regulations						✓		
Continued infringements of the above, following previous warnings or sanctions								✓

Response to an Incident of Concern



Contact Details

Schools Designated Child Protection Officer: Mrs Jenny Hunt
School eSafety Co-ordinator: Mrs Lois Mundy
19

Approved by the Governing Body on _____

Chair of Governors_____ Head teacher_____

Appendices

- Pupil Acceptable Usage Policy template
- Staff and Volunteers Acceptable Usage Policy template
- Parents / Carers Acceptable Usage Policy Agreement template
- Use of Digital Images Consent Form
- Mobile Phone Use
- Questions for Schools to consider
- Links to other organisations, documents and resources
- Legislation

Pupil Acceptable Use Policy – Years 4 - 6

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people 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.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils 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.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password with anyone or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology to support our education:

- I understand that the school ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will 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.
- I will not take or distribute images of anyone without their permission.

I understand that the school has a responsibility to keep the technology secure and safe:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not 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.
- 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.
- I will only use chat and social networking sites in school.

When using the internet for research for my school work, I understand that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

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

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this is cyber bullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action. This may include loss of access to the school network / internet, visits to behaviour room, suspensions, contact with parents, and, in the event of illegal activities, involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

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 in school (when allowed) eg mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

Name of Pupil

Signed

Date

Class

Acceptable Use Policy – Years 1 - 3

This is how we stay safe when we use computers:

I will ask a an adult if I want to use the computer

I will only use activities that an adult has told or allowed me to use.

I will take care of the computer and other equipment

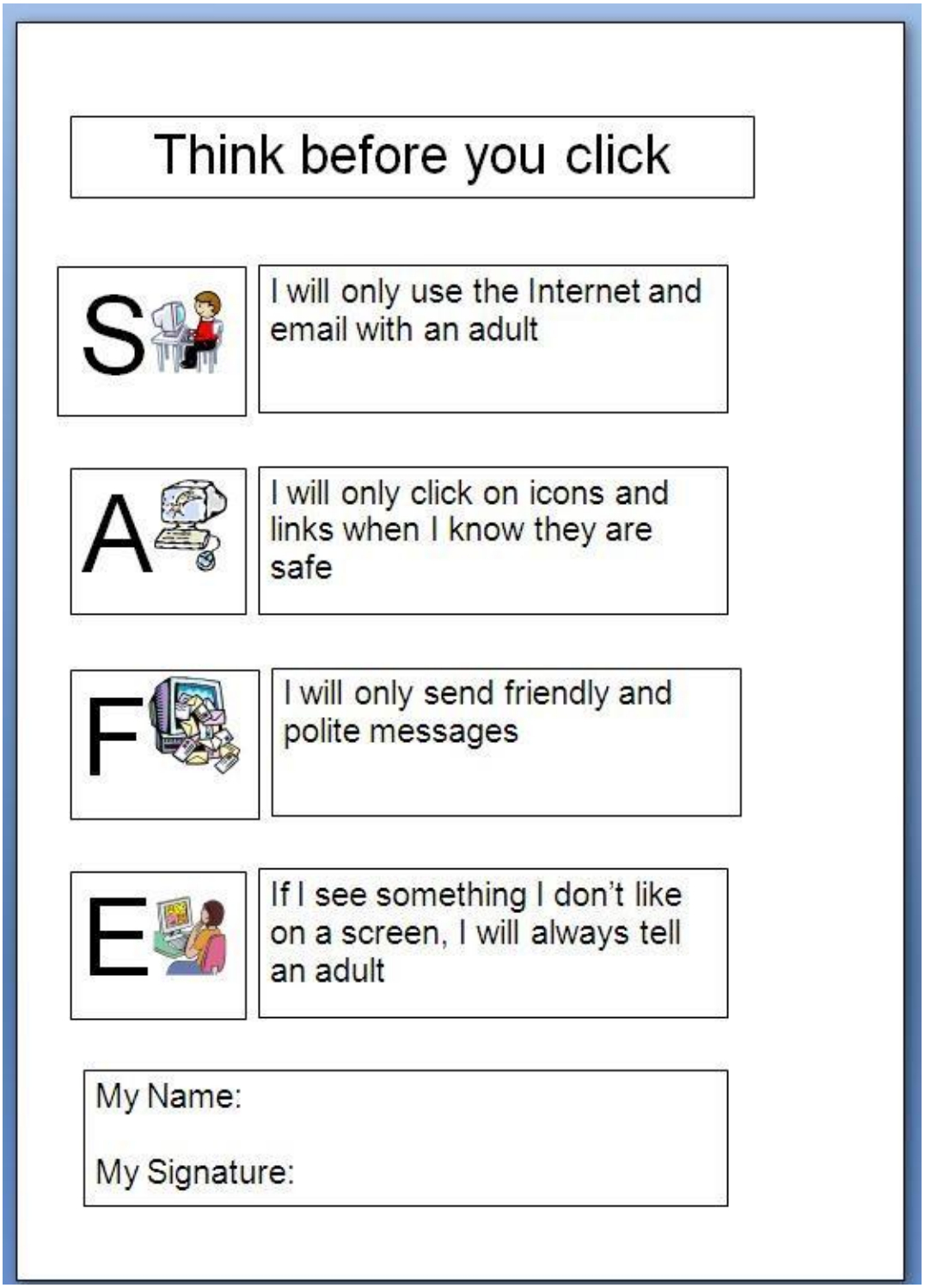
I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I will tell an adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Acceptable Use Policy – EYFS



Staff Acceptable Use Policy

Guidance for Use

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained and the safety of all users is ensured. Members of staff are entitled to seek their own legal advice on this matter before signing the AUP.

In order to protect staff members it is essential to have an AUP in place which has been viewed and understood. All employees (including teaching and non-teaching staff) must be aware of the school rules for use of information systems and professional conduct online whether on or off site. Misuse of ICT systems and other professional misconduct rules for employees are specific and instances resulting in disciplinary procedures or staff dismissal can and will occur.

With internet use becoming more prominent in every day life for personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements). It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis. All members of staff should read, understand and sign the AUP before being granted access to any of the schools' ICT systems.

Social Media

We are aware that we cannot ban staff from using sites in their own personal time. However, we can put in place appropriate guidance and boundaries around staff interaction with pupils (past or present) and parents. It is recommended that any contact with pupils and parents only takes place via school approved communication channels (e.g. school email address, the school learning platform or Class Dojos), so it can be monitored and traced in the case of an allegation or concern. However, we recognise that in some cases there may be pre-existing relationships which mean that any "ban" from adding parents as friends or contacts on personal social networking sites may be difficult to enforce. However, staff should be aware that they must conduct themselves in a professional manner at all times in using social media to communicate with parents and must not bring the school into disrepute. Breach of this may lead to disciplinary action being taken.

Use of Equipment

Occasional personal use of the school's computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However, this is at the school's discretion and can be revoked at any time. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP.

Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with

intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (a strong password has numbers, letters and symbols, with 8 or more characters and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware, without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace or accessed remotely. Any data which is being removed from the school site (such as via email) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.
- I have read and understood the school eSafety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Co-ordinator (Mrs J Hunt) and/or the eSafety Co-ordinator (Mrs L Mundy) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the eSafety Coordinator or the designated lead for filtering (Mr M Haworth) as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the ICT Support Provider/Team (Mr M Haworth and Mrs L Mundy) as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.).

- I will promote eSafety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the eSafety Co-ordinator (Mrs L Mundy) or the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood the Staff ICT Acceptable Use Policy. Signed:

…….... Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

Parent / Carer Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet, and other digital information and communications technologies, are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people 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 parents and carers are aware of the importance of eSafety 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 the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

Permission Form

Parent / Carers Name

Pupil Name

- As the parent / carer of the above pupil, I give permission for my child to have supervised access to the internet and to ICT systems at school.
- I know that my child has signed an Acceptable Use Agreement and has received, or will receive, eSafety education to help them understand the importance of safe use of ICT – both in and out of 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 child'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 Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's eSafety.

Signed

Date

Use of Photographs, videos and other images within School

This applies to all staff, volunteers and students on work placement.

There are a number of things that you need to address when using images of people, especially children, some of which is contained in the Data Protection Act 1998:

- You must get the consent of all parents of children appearing in the photograph or video/DVD image before it is created
- You must be clear why and what you'll be using the image for and who will see it
- If you use images from another agency, you need to check that the agency has obtained informed consent Safeguarding issues:
- Use equipment provided by the school to take the images and not personal devices
- Download and store images in a password protected area of the school network not on personal computers
- When images are stored on the system they should be erased immediately from their initial storage location e.g. camera
- Don't use full names or personal contact details of the subject of any image you use

- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner
- No images of a looked after child should be created or used without prior consent from Children's Social Care
- Don't use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use
- Always destroy images once consent has expired or the child has left your school

Consider:

- Are CCTV (security) cameras sited where they may compromise the privacy of individuals?
- How public are your display boards?
- What is the purpose and audience of video's and DVD's you have created?
  - Are all of your images and media securely

stored at your school?

- Images on websites, and other publicity can become public and outside your control Any implications of using images offsite
- The press are exempt from the Data Protection Act, if you invite them to your premises or event, you need to obtain prior consent from parents of children involved
- Including images from different ethnic groups and those of disabled children
- Check out any copyright implications

The Information Commissioner's Office guidance advises that photographs taken for personal use e.g. by parents at special events, at an education setting are not covered by the Data Protection Act.

Useful links/resources:

- Photographs and Videos, Information Commissioners Office, at: http://www.ico.gov.uk/for_the_public/topic_specific_guides/schools/photos.aspx

Digital Images Consent Form

Using images of children in High View Primary Learning Centre

Name of the child's parent / carer:

Name of child: Class:

Occasionally, we may take photographs of the children at our school. We use photographs as evidence of learning, part of observations and development records (learning journeys). We may also use these images

in our prosp ectus or in other printed publications that we produce, as well as on our website. We may also make video/DVD recordings for monitoring events or other educational use.

In the event of our school being visited by the media who may take photographs or film footage of an event, children and young people may appear in these images, which may appear in local or national newspapers, or on televised news programmes, no personal details to identify a child will be provided with the images.

Photographs published on public websites will not have any personal details published with them that could be used to identify a child.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please answer questions 1 to 5 below, then sign and date the form where shown.

Please return the completed form to the setting as soon as possible.

1) May we use your child's photograph in our prospectus and other printed publications for promotional purposes? Yes/No

2) May we put your child's image on our website? Yes/No

3) May we record your child's image on video/DVD? Yes/No

4) Are you happy for your child to appear in the media? Yes/No

5) May we use your child's image in our school newsletter? Yes/No

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.
I have read and understood the conditions of use.

Parent's or guardian's signature: Name (in block capitals):

Date

If circumstances change that could impact on your child's safety and security, please inform the School immediately.

Dear Parent / Carer,

We discourage children from brining their mobile phones to school, as they can pose a risk to the safety of the child, staff and other children at our school. However, in special circumstances, we know that it can be necessary for some children to have their phone on the premises. In these cases, we require both the parent and child sign the attached policy, and therefore agree to abide by it.

Yours faithfully,

Mrs J Hunt

Pupil's Name: _____ Class: _____

Pupils' Mobile Phones in School Policy

High View Primary Learning Centre

Pupils may only bring their mobile phone to school in special circumstances, with the permission of their class teacher and their parents. In these cases, this agreement must be signed and agreed to by the child and the parent.

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used within the school site, must be turned off before entering it and not turned on again until outside the school gate.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in to the child's class teacher should they be brought into school.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy. After this, the pupil involved will no longer have permission to bring the device onto school premises.

I have read the above policy and agree to abide by it.

Signed (parent / carer): _____ Date : _____

Signed (pupil): _____ Date : _____

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Sheffield Safeguarding Children Board http://www.safeguardingsheffieldchildren.org.uk

Safer Internet Centre: http://www.saferinternet.org.uk/

UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis

CEOP - Think U Know - http://www.thinkuknow.co.uk/

Childnet - http://www.childnet.com

Netsmartz http://www.netsmartz.org/index.aspx

Teach Today http://www.teachtoday.eu/

Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/

Byron Review ("Safer Children in a Digital World")
http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/

Guidance for safer working practice for adults that work with children and young people -
http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resourcesand-practice/ig00311/

Information Commissioners Office/education:
http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

ICO guidance on use of photos in schools:
http://www.ico.gov.uk/youth/sitecore/content/Home/for_the_public/topic_specific_guides/schools/photos.aspx

Ofsted survey: http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-allby/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB

Plymouth Early Years ESafety Toolkit:
http://www.plymouth.gov.uk/early_years_toolkit.pdf

Protecting your personal information online:
http://www.ico.gov.uk/~/media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx

Getnetwise privacy guidance: http://privacy.getnetwise.org/

Children and Parents

Vodafone Parents Guide: http://parents.vodafone.com/

NSPCC: http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internetsafety/internet-safety_wdh72864.html

Google guidance for parents: http://www.teachparentstech.org/

E-Parenting tutorials: http://media-awareness.ca/english/parents/internet/eparenting.cfm

Practical Participation – Tim Davies: http://www.practicalparticipation.co.uk/yes/

Digital Citizenship: http://www.digizen.org.uk/

Kent “Safer Practice with Technology”:
http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-withtechnology-for-school-staff.aspx

Connect Safely Parents Guide to Facebook:
http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html

Ofcom – Help your children to manage the media:
http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-theirmedia/

Mobile broadband guidance: http://www.mobile-broadband.org.uk/guides/complete-resource-ofinternet-safety-for-kids/

Orange Parents Guide to the Internet: http://www.orange.co.uk/communicate/safety/10948.htm

O2 Parents Guide: http://www.o2.co.uk/parents

FOSI – Family Online Internet Safety Contract: http://www.fosi.org/resources/257-fosi-safetycontract.html

Cybermentors (Beat Bullying): http://www.cybermentors.org.uk/

Teachernet Cyber bullying guidance:
http://www.digizen.org/resources/cyber bullying/overview

“Safe to Learn – embedding anti-bullying work in schools” http://www.anti-bullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law,_policy_and_guidance/safe_to_learn.aspx

Anti-Bullying Network - http://www.antibullying.net/cyber bullying1.htm

Cyber bullying.org - http://www.cyber bullying.org/

CBBC – stay safe: http://www.bbc.co.uk/cbbc/help/home/

Technology

Kaspersky – advice on keeping children safe -
http://www.kaspersky.co.uk/keeping_children_safe

Kaspersky - password advice: www.kaspersky.co.uk/passwords

CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/

Which Parental control guidance: http://www.which.co.uk/baby-and-child/child-safety-athome/guides/parental-control-software/

How to encrypt files: http://www.dummies.com/how-to/content/how-to-encrypt-important-filesor-folders-on-your-.html

Get safe on line – Beginners Guide -

http://www.getsafeonline.org/ngcontent.cfm?a_name=beginners_1

Childnet Parents and Teachers on downloading / music, film, TV and the internet - http://www.childnet.com/downloading/

Microsoft Family safety software: http://windows.microsoft.com/en-US/windowsvista/Protecting-your-kids-with-Family-Safety

Norton Online Family: https://onlinefamily.norton.com/

Forensic Software http://www.forensicsoftware.co.uk/education/clients.aspx

Legislation
Schools should be aware of the legislative framework under which this ESafety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence
to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities; • Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.
Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to: • Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system; • Prevent or detect crime or in the interests of national security;

- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a

position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include: • The right to a fair trial

- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

High View Primary Learning Centre would like to acknowledge Sheffield Safeguarding Children Board for the use of their example documentation, which was used to compose this policy.

SSCB would like to acknowledge YHGfL, SWGfL and Kent County Council for the use of their documentation.