Version	Sept 2020
Owner	Skelton Primary School
Approved	
Review Cycle	1 year
Next Review	Sept 2021

Online Safety 2021

Skelton Primary School offers a positive, safe learning environment for its community, in which everyone has equal and individual recognition and respect. We celebrate success and are committed to the continuous improvement and fulfilment of potential in every child.

We encourage increasing independence and self-discipline amongst the pupils. Everyone within the school has an important role to play in sharing responsibility for the development of positive behaviour and attitudes.

Contents

Introduction 3
Scope of Policy
Development/ Monitoring/ Review
Schedule for development/ monitoring review 4
Comunication of this Policy
Roles & responisibilties 6
Use of digital & video images 12
Managing IT systems and access 13
Filtering and internet access
Passwords 14
Management of Access 15
Data Protection
Fax 17
Commmuncations Technology 18
Unsuitable/ inappropriate activities 19
Responding to incidents of misuse 20
Response to incidents of concern 25

APPENDICES

__IT Acceptable Use for Children__
Parent Consent Form- photographs/ videos
Parent Consent Form- internet use

__Staff and Volunteer Agreed useage__
Social Media/ Networking Policy

1. POLICY INTRODUCTION

Digital technologies have become integral to the lives of young people, both within education and outside. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people have an entitlement to safe Internet access at all times.

The S.P.S. Online Safety policy encompasses the necessary measures to ensure that risks associated with internet use are carefully managed and reduced, helping all users to be responsible and enabling them to stay safe while accessing the Internet and other communication technologies for educational and personal use.

2. SCOPE OF POLICY

- This policy applies to all members of the S.P.S. family (including staff, children, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of our school IT systems, both in and out of the school.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students 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 online safeguarding 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 S.P.S. 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 within school.
- S.P.S. will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

3. DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

Online safety procedures are developed in dialogue with Team, Staff and Governor meetings and in consultation with parents, carers directly through the website and Friday Flyers.

4. SCHEDULE FOR DEVELOPMENT/ MONITORING/ REVIEW

Title	Online Safety Policy
Version	1
Date	Autumn 2020
Author	Sarah Walker
Approved by Governors	Autumn 2020
Monitoring period	annually
Reported on to Governors	termly
Should safeguarding incidents take place, the following external persons/ agencies should be informed	LADO if staff member Pam Gartland Safeguarding First for advice
Policy will be monitored using	SIMs logs CPOMs Internal monitoring data Survey findings of children, parents/ carers and staff

5. COMMUNICATION OF THE POLICY

The Online Safety Policy will be distributed to staff and governors. It will be available to parents and children on the website. It will be communicated to children through the IT lessons, School Council and assemblies. Key messages from the policy will be displayed around S.P.S. Any amendments will be shared with all stakeholders on the website and alerts will be sent by text/email and through internal meetings to ensure awareness.

- S.P.S. senior leadership team will be responsible for ensuring all members of staff and students are aware of the existence and contents of the Online Safety policy and the use of any new technology within school.
- The Online Safety 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 members of the S.P.S. community.
- Online Safety training will be part of annual transition programme regarding the children's responsibilities.
- Pertinent points from the Online Safety policy will be reinforced across the curriculum and across all subject areas when using IT equipment within Skelton.
- The key messages contained within the Online Safety policy will be reflected and consistent within all acceptable use policies in place.
- S.P.S. embeds Online Safety messages across the curriculum whenever the Internet or related technologies are used.

- The Online Safety policy will be introduced to the children at the start of each school year.
- Safeguarding posters will be prominently displayed around school by IT lead.

6. ROLES AND RESPONSIBILITIES

We believe that Online Safety 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 teaching and learning.

Responsibilities of the Senior Leadership Team

- The Headteacher has overall responsibility for Online Safety, all members of the school community, though the day-to-day responsibility for Onlien Safety will be delegated to the IT lead.
- The Headteacher and senior leadership team are responsible for ensuring that IT lead and all staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues when necessary.
- The Headteacher and senior leadership team will ensure that there is a mechanism in place (regular line-management meetings) to allow for monitoring and support of those at S.P.S. who carry out the internal Online Saefty monitoring role.
- The Designated Safeguarding Team will receive monitoring reports via CPOMs of any online safety incidents.

Responsibilities of the Online Safety Lead

- To promote an awareness and commitment to Online Safety.
- To be the first point of contact, alongside SLT on all Online Safety matters.
- To take day-to-day responsibility for Online Safety and support in establishing and reviewing the Online Safety policies and procedures.
- To communicate regularly with S.P.S. technical staff and the designated Safeguarding governor
- To develop an understanding of current Online Safety issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online Safety issues.
- To ensure that Online Safety education is embedded across the curriculum.
- To ensure that Online Safety is promoted to parents and carers.
- To liaise with the local authority, the Safeguarding Partnership, the NGfl and other relevant agencies as appropriate.
- To monitor and report on Online Safety issues to the Designated Safeguarding Team as appropriate and the senior leadership team termly.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.
- To ensure that CPOMS incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote S.P.S. safeguarding policies and guidance.
- To read, understand and adhere to the S.P.S. staff Acceptable Use Policy.
- To report any suspected misuse or problem to the I.T. lead or SLT.
- To develop and maintain an awareness of current safeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with students should be on a professional level and only through S.P.S. based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.

- To embed safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide students carefully when engaged in learning activities involving technology.
- To ensure that students 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 safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To ensure electronic platforms, such as CPOMS and email accounts, are logged off when not in use.
- To understand and be aware of incident-reporting mechanisms which exist within S.P.S.
- To maintain a professional level of conduct in personal use of technology at all times.
- 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 S.P.S. safeguarding policies and guidance.
- To read, understand and adhere to the S.P.S. staff Acceptable Use Policy.
- To report any safeguarding related issues arise to the I.T lead or SLT.
- To develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support S.P.S. in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised and restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for protecting the security of S.P.S.' I.T system.
- To liaise with appropriate people and organisations on technical issues.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on S.P.S.-owned devices.
- 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 S.P.S.-owned software assets is restricted.

Protecting the professional identify of all staff, work placement students, guests and volunteers

Communication between adults and children / young people, 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, blogs etc.

When using digital communications, staff and volunteers should:

- Only make contact with young people for professional reasons and in accordance with the policies and professional guidance of S.P.S. When emailing students staff should copy in a colleague or line manager. Only school approved communication methods should be used- email and Microsoft Teams for Remote Learning.
- Not share any personal information with a child e.g. should not give their personal contact details to young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the young person, other than that which might be appropriate as part of their professional role, or if the young person is at immediate risk of harm.
- Not send or accept a friend request from the 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 young people so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring S.P.S. into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Designated Safeguarding Lead

- 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 cyberbullying and the use of social media for this purpose.

Responsibilities of Children

- To read, understand and adhere to the S.P.S. Acceptable Use Policy for Children.
- To help and support S.P.S. in the creation of Online Safety 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 regarding online bullying.
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in the 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 the school and at home, including judging the risks posed by the personal technology owned and used outside the school.
- To ensure they respect the feelings, rights, values and intellectual property of others, in their use of technology in the school and at home.
- To understand what action they should do if they feel worried, uncomfortable, vulnerable or at risk while using technology in the 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 S.P.S.
- To discuss Online Safety issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support S.P.S. in promoting Online Safety .
- To read, understand and promote the S.P.S. 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 Online Safety 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 school if they have any concerns about their children's use of technology.
- To agree to and sign the 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. I will:

- *Not share images taken at school of children other my own on social media nor will I make comments that may upset or offend members of school community.*
- *Read through and sign the Student IT Acceptable Use Policy on behalf of my child.*

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote S.P.S. Online Safety policies and guidance.
- To develop an overview of the benefits and risks of the Internet and common technologies used by students.
- To develop an overview of how the S.P.S. I.T infrastructure provides safe access to the Internet.
- To develop an overview of how S.P.S. encourages students to adopt safe and responsible behaviours in their use of technology, in and outside of school.

- To ensure appropriate funding and resources are available for the school to implement its Online Safety strategy.

The role of the Safeguarding Governor includes:

- regular meetings with the IT/ Online Safety lead
- reporting to Governors meeting

Responsibilities of Other Community / External Users:

- S.P.S. will liaise with local organisations to establish a common approach to Online Safety and the safe use of technologies.
- S.P.S. will be sensitive and show empathy to internet-related issues experienced by students out of school, e.g. social networking sites, and offer advice where appropriate.
- S.P.S. will provide an I.T Acceptable Use Policy for any members of external organisations, guests or visitor etc. who needs to access S.P.S. computer system or Internet on school grounds.
- Any members of external organisations, guests or visitor etc. will sign an I.T Acceptable Use Policy, prior to using any equipment or the Internet within the school.
- S.P.S. will ensure that appropriate levels of supervision exist when external organisations make use of the Internet and I.T equipment within school.

Education - Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in Online Safety is therefore an essential part of the S.P.S. Online Safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- We will provide a series of specific Online Safety related lessons in specific year groups as part of the computing curriculum.
- We will celebrate and promote Online Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant Online Safety messages with students 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.
- Children will be taught how to use a range of age-appropriate online tools in a safe and effective way.

- We will remind children about their responsibilities through the I.T Acceptable Use Policy for Children which every child will commit to.
  Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach children 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, search engines will be set to 'Safe Search' so that only appropriate content is accessed. All use will be monitored and students will be reminded of what to do, if they come across unsuitable content.
- All children will be taught 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.
- Children will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
- Children 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 Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety will be made available to staff.
- An audit of the Online Safety training needs of all staff will be carried out regularly.
- All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand S.P.S. Online Safety policy and IT Acceptable Use Policies.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff and team meetings

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 I.T than their children. S.P.S. will therefore take every opportunity to help parents understand these issues through:

- parents' evenings
- class assemblies
- newsletters
- letters

- website
- information about national / local Online Safety campaigns / literature

7. USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and children 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.
S.P.S. 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 children 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 e.g. 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; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others, without their permission.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained in the Social media consent form (see appendix) before photographs of students are published on the school website or elsewhere. Children's work can only be published with the permission of the student and parents or carers.
- When searching for images, video or sound clips, children will be taught about copyright and acknowledging ownership.

8. MANAGING IT SYSTEMS AND ACCESS

- S.P.S. will be responsible for ensuring that access to the I.T systems is as safe and secure as reasonably possible.
- 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 required.

- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- S.P.S. will agree which users should and should not have Internet access and the appropriate level of access and supervision they should receive.
- Members of staff will access the Internet using an individual username and password, which they will keep secure. They will ensure that they log out, or lock the computer after each session and will not allow students to access the Internet through their username and password. They will abide by the S.P.S. I.T Authorised User Policy at all times.

9. FILTERING INTERNET ACCESS

- S.P.S uses a filtered Internet service called Smoothwall
- S.P.S. Internet provision includes filtering appropriate to the age and maturity of students.
- S.P.S. will always be proactive regarding the nature of content, which can be viewed through the S.P.S. Internet provision.

  S.P.S. has a clearly defined procedure for reporting breaches of filtering. All staff and students will be aware of this procedure by reading and signing the I.T 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 I.T lead or SLT. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the I.T lead of SLT. S.P.S. will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- S.P.S. will regularly review the filtering product for its effectiveness.
- The filtering system will block all sites on the Internet Watch Foundation list as well as any Sites the Local Authorty deem inappropriate in the their top lever filter 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 by IT Network Manager.
- Our children will be taught to assess content as their Internet usage skills develop.
- Our children 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.

10. PASSWORDS

- A secure and robust username and password convention exists for all system access, i.e. email, network access, school management information systems etc.
- All staff will have a unique, individually named user account and password for access to I.T equipment and information systems available within S.P.S.
- All information systems require end users to change their password at first log on.
- Users are prompted to change their passwords at pre-arranged intervals, or at any time that they feel their password may have been compromised.

- Users should change their passwords whenever there is any indication of possible system or password compromise.
- All staff and children 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 students will have appropriate awareness training on protecting access to their personal username and passwords for IT access.
- All staff and children will sign an Acceptable Use Policy prior to being given access to IT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
  - Do not write down system passwords.
  - Only disclose your personal password to authorised IT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
  - Always use your own personal passwords to access computer-based services, never share these with other users.
  - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
  - Never save system-based usernames and passwords 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 protection policy. S.P.S. 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 special characters in their passwords (! @ # $ % * ( ) - + = , < > : : “ ‘): the more randomly they are placed, the more secure they are.

11. MANAGEMENT OF ASSETS

- Details of all S.P.S.-owned hardware will be recorded in a hardware inventory.
- All redundant IT 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 IT 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. S.P.S. will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any IT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

12. DATA PROTECTION

Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 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.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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.
- Transfer data using encryption and secure password-protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - The data must be encrypted and password protected
  - The device must be password protected
  - The device must offer approved virus and malware checking software
  - The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- S.P.S. has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school. S.P.S. 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 will be controlled appropriately through technical and non-technical access controls.
- Users should be 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 (Senior Information Risk Officer – the Headteacher) and the applicable IAO (the Information Asset Owner)
- All access to the S.P.S. information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on school servers shall be 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 or IAO.

- Staff and students will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- 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.

13. FAX

- Fax machine is located in the main office.
- Only school staff should have direct access to the Fax machine.
- Sensitive or personal information must not be included within a Fax itself, as the information may be insecure. Such information should be enclosed in a document (e.g. Word document) then encrypted and password protected and should then be sent as an attachment to an email, with the password communicated by telephone.

14. COMMUNICATION TECHNOLOGIES

A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff & other adults				Children			
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 can be brought into school	*				**stored securely by office.*			
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones or other camera devices	*T							*
Use of tablets, IPAds etc	*T							*
Use of personal email addresses on school OR on school network				*				*
Use of school email for personal use				*				*
Use of chat rooms/ facilities				*				*
Use of instant messaging				*				*
Use of social networking sites	*T							*
Use of blogs	*T			*				*

T = Only on authorised S.P.S. equipment and systems, used solely in connection with teaching and learning within the school.

When using communication technologies S.P.S. considers the following as good practice:

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

15. UNSUITABLE / INAPPROPRIATE ACTIVITIES

S.P.S. believes that the activities referred to in the following section would be inappropriate in the school context and that users, as defined below, should not engage in these activities in school or outside when using school equipment or systems. S.P.S. policy restricts certain Internet usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for certain uses	Unacceptable	Unacceptable & illegal
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, e.g. under the child protection, obscenity, computer misuse and fraud legislation**					*
• **adult material that potentially breaches the Obscene Publications Act in the UK**					*
• **criminally racist material**					*
• **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 Academy systems to run a private business				*	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by NGfL and / or the Academy or Local Authority				*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					*

Creating or propagating computer viruses or other harmful files					*
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				*	
On-line gaming				*	
Online gambling				*	
Online shopping/ commerce			*T		
File sharing			*T		
Use of social networking sites			*T	*	
Use of video broadcasting eg Youtube		*T			

T = Only on authorised S.P.S. equipment and systems, used solely in connection with teaching and learning within school.

16. RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of IT, 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

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 an appropriate 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.

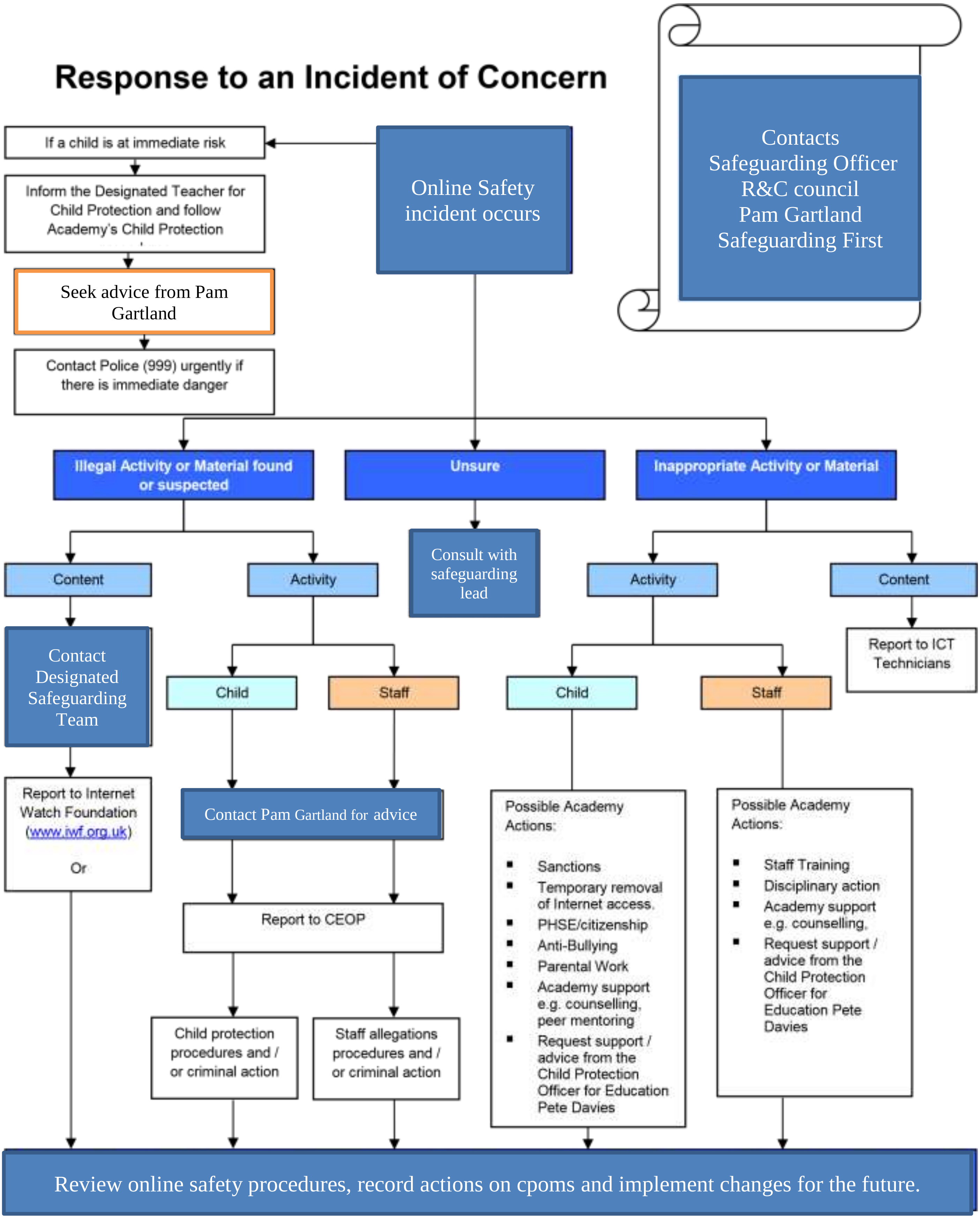
STUDENT Incidents	Refer to Class teacher	Refer to SLT	Refer to HT	Refer to Police	CPOMs reported	Refer to IT technician for filtering/ security etc	Inform parents/ carers	Removal of network / internet access rights	Warning	Further more serious sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			*	*						
Unauthorised use of non-educational sites during lessons	*				*					
Unauthorised use of mobile phone / digital camera / other handheld device	*	*					*			*
Unauthorised use of social networking / instant messaging / personal email	*				*					
Unauthorised downloading or uploading of files		*			*		*			*
Allowing others to access school network by sharing username and passwords		*			*		*			
Allowing others to access school network by sharing username and passwords		*			*		*			
Attempting to access or accessing the schoolnetwork, using another student's / pupil's account		*			*		*		*	
Attempting to access or accessing the Academy network, using the account of a member of staff		*			*		*	*		
Corrupting or destroying the data of other users		*			*		*	*		
Sending an email, text or social media post 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 S.P.S.		*	*		*		*	*		*
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

INCIDENTS

	Refer to line manager	Refer to HT	Refer to LA/ HR	Refer to police	Refer to tech support for action	Warning	Suspension	Disciplinary
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 S.P.S. network, using another person's account		*						*
Careless use of personal data e.g. holding or transferring data in an insecure manner	*					*		*
Deliberate actions to breach data protection or network security rules		*						*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		*						*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		*						*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / students		*						*
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 S.P.S		*						*
Using proxy sites or other means to subvert the school 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



Online Safety incident occurs

Contacts
Safeguarding Officer
R&C council
Pam Gartland
Safeguarding First

If a child is at immediate risk

Inform the Designated Teacher for Child Protection and follow Academy's Child Protection

Seek advice from Pam Gartland

Contact Police (999) urgently if there is immediate danger

Illegal Activity or Material found or suspected

Unsure

Inappropriate Activity or Material

Content

Activity

Consult with safeguarding lead

Activity

Content

Contact Designated Safeguarding Team

Child

Staff

Child

Staff

Report to ICT Technicians

Report to Internet Watch Foundation (www.iwf.org.uk)

Or

Contact Pam Gartland for advice

Report to CEOP

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Possible Academy Actions:

- Sanctions
- Temporary removal of Internet access.
- PHSE/citizenship
- Anti-Bullying
- Parental Work
- Academy support e.g. counselling, peer mentoring
- Request support / advice from the Child Protection Officer for Education Pete Davies

Possible Academy Actions:

- Staff Training
- Disciplinary action
- Academy support e.g. counselling.
- Request support / advice from the Child Protection Officer for Education Pete Davies

Review online safety procedures, record actions on cpoms and implement changes for the future.

CONTACT DETAILS	
S.P.S. Nominated Person	Andy Woolf (AHT) Sarah Walker (HT)
S.P.S. Computing Lead	Mrs Sayer (Y4 Team Leader)
S.P.S. IT Network Manager	Chris Clements
Child Protection Officer	LA Link Officer (01642 774774) Pam Gartland Safeguarding First

APPENDICES

Student IT Acceptable Use A
Parent Consent Form- photographs/ videos B
Parent Consent Form- internet use C

Staff and Volunteer Agreed Useage Policy D
Social Media/ Networking Policy E

APP A

IT ACCEPTABLE USE POLICY
For Children

As part of our commitment to provide the best teaching and learning opportunities for our students, particularly when using IT, it is necessary to ask our children to use the Skelton computer systems in a safe and responsible manner.

The computer systems provided by Skelton Primary School offer safe, secure and reliable access to a number of services:

- A range of IT systems, including computers, laptops, iPads, iPods etc.
- A wide range of educational and Office software
- Printing and scanning
- Internet access
- Data storage
- E-mail

All of these facilities are available to our children and in order to make them safe, secure and reliable we have a number of measures in place, such as:

- Log on usernames and passwords
- Data storage and backup systems
- E-Safe security monitoring
- Antivirus software
- Web filtering
- Firewall

At Skelton Primary School we do all that we can to keep students safe when using any of our IT systems, but it is expected that you will also help us by making sure that you follow all of the advice given, including staying safe when using the Internet. This way we can work together to keep you and our computer systems safe and enable you to get the most out of IT to help you with your learning.

So that we can make our IT systems as safe and secure as possible, a list of rules must be followed. Keeping to these rules will ensure that we can continue to provide quality IT facilities that you, our children deserve.

S.P.S. will ensure good access to IT to enhance learning and in return, expect the children to be responsible users as outlined below:

RULES FOR SAFE & RESPONSIBLE USE OF IT

For my own personal safety: I know that irresponsible use of IT systems may result in the loss of computer, printing, emails and/ or internet access either on a temporary or permanent basis and that punishment may follow.

I will:

- Log onto all school computer systems using only my own username and password and I will not share this information with anyone else.
- Only use school computer systems, e-mail and Internet access that are appropriate to my education.
- Only use IT equipment that is supplied to me by the school.
- Access the school's wireless system with school IT equipment only.
- Always get permission from a teacher or a member of staff before using any portable storage device such as a CD, DVD, USB pen or portable hard drive and have them scanned with anti-virus software.
- Use all media responsibly, carefully and politely and will not write anything that I would not put in a letter or note, as it can easily be copied, forwarded, or sent to the wrong person by mistake and I know that I am responsible for all e-mails I send and contacts I make.
- Treat the equipment with respect, as I know that any deliberate damaging of equipment will not be tolerated, will be charged for and a punishment given.
- Take sound recordings, pictures or videos on school equipment only and then only with permission from a teacher or a member of staff.
- Only make sound recordings, pictures or videos, if the person involved gives their consent.
- Be aware of 'stranger danger' when I am communicating on line.
- Report to a teacher or member of staff any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I am on line.
- Be aware that when using the Internet to find information, that it may not be accurate or correct.

I will not:

- Post any of my personal details or images on a website, blog, or in an e-mail etc. unless authorised to do so by a teacher, or a member of staff.
- Send or try to look at, save, print, or show offensive messages or pictures on any of the school's IT systems. If any of these accidentally come on my screen, I will inform my teacher immediately.
- Access, move, delete or in any way change anyone else's work.
- Attempt to fix a problem myself, but will inform a teacher or member of staff if I find anything wrong with any IT equipment.
- Run any programs, games etc. on any of the school IT systems, from portable storage devices such as a USB pen, hard drive, MP3 player etc.
- Use or attempt to use a mobile phone whilst in the school.
- Use or try to use public chat rooms, blogs or social networking sites whilst in the school.

- Use or connect to any Bluetooth device on any school systems.
- Look or try to look at adult, racist, homophobic or other offensive or illegal material.
- Use IT systems for online bullying, racial or homophobic harassment or intimidation.
- Use social media in a way that will be offensive or threatening to others.

Always be **WISE** when using the Internet
WHY would someone want your personal information?
Be **INSPIRED** as the Internet offers great tools to help you learn.
Be **SECURE** online.
EVALUATE what you see on the Internet, as it is not always true.

In circumstances where the school's IT systems have allegedly been used for storing text or images that are unauthorised or unlawful, or for criminal purposes, S.P.S. will exercise its right by electronic means to monitor the use of the school's IT systems. This includes the monitoring of documents, Internet use, the interception of e-mails and the deletion of inappropriate materials from our IT systems.

Please take time to discuss the above document with your child and then complete, sign and return to your child's class teacher

Child: …………………………………………………Class:…………………………

Pupil's Agreement

I have read and understood Skelton Primary School's IT Acceptable Use Policy for Children. I will use the IT systems and Internet in a responsible way and obey these rules at all times. I understand that I will be expected to pay for any damage I cause to equipment.

Signature of child: ……………………………………Date: ………………………………..

APP B

Skelton Primary School Media Consent Form

Your Consent Preferences

This form has been written to give you choice and control over how our school uses some of your personal data.

You may withdraw these consent preferences at any time. Further information about how to do this can be found below.

Non-Essential Communications The school will want to contact you to tell you about school events, news, and general updates. Please state if you would like to receive these communications. Eg Friday Flyer etc If so, please tick which apply.	**YES**		**NO**	
	HARD COPY	**EMAIL**		
If you require communication by email please provide email details:				

School's use of images:

In Skelton Primary School, digital media is vital to record the child's learning journey and help celebrate their achievements.

If you wish to give consent to some, but not all of these areas, please tick those which you consent to.

Images may be used for:

- ○ Display
- ○ Evidencing key moments in learning
- ○ Group/ class photos
- ○ School's online presence- Website, Blog, official School Facebook page, Friday Flyer
- ○ External media events- Press, TV, Radio

Skelton Primary School is keen to celebrate your children's success with you but also recognises the risks of keeping children safe in an online world.

We will therefore reduce any risks by using as few identifiable factors as possible. Images may be uncaptioned or only use first names etc.

Photos and Videos **I consent to school using images and videos of my child to ensure the needs of the school and curriculum are met.**	**YES**	**NO**

Parent/Guardian Name:	Parent's Signature:
Pupil Name:	
Date:	

To withdraw or change your consent preferences please contact:
The office manager at school or office@skeltonprimaryschool.co.uk

APP C

Parent's Consent for Internet Access

I have read and understand Skelton Primary School's 'rules for safe and responsible use of IT and give permission for my son/daughter to access the Internet.

I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials and I agree that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that the school is not liable for any damages arising from use of the Internet facilities.

We will support the Academy 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.

I understand that we 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

I understand that I will be charged if my son/daughter damages any IT equipment.

Signature of Parent/Carer: ……………………………………………………………………….

Please print name: …………………………………………….Date…………………………….

APP D

IT Agreed Usage Policy for Staff

As part of our commitment to provide the best Teaching and Learning opportunity for our children, particularly when using IT, a wide range of facilities are made available to staff to assist them in delivering their Teaching through IT. It is however, necessary that we ask all our staff to use our computer systems in a safe and responsible manner.

The computer systems owned by Skelton Primary School offers safe, secure and reliable access to a number of services:-

- E-mail
- Data storage
- Internet access
- Printing, scanning & copying
- A Virtual Learning Environment
- A wide range of educational & office software

All of these facilities are available for our staff to utilise, but in order to make them safe, secure and reliable we have a number of measures in place, such as: -

- Secure Data Storage & Backup Systems
- Logon Usernames and Passwords
- Anti-Virus Software
- Web Filtering
- Firewall

It is staff's responsibility to ensure that electronic platforms, such as S.P.S logins, CPOMs and email accounts, are correctly logged out when not in use to ensure the safety of both pupils and staff is maintained.

To maintain a safe and secure IT environment, an Agreed Usage Policy must be enforced. Adherence to this policy will ensure that we can continue to provide the level of service that our students deserve and that our staff have come to expect.

All Staff who intend to use the Academy IT Network and access any of the Academy systems, i.e. SIMS, E-mail, VLE, Printing etc. must comply with this IT Acceptable Use Policy (AUP) and sign an AUP Consent Form.

Unlawful and Illegal Use

The Skelton Primary School IT Network (LAN) and associated services may be used for lawful purposes only.

As a user of the Academy IT systems you agree not to send or receive materials or data that is n violation of any law or regulation which :

- constitutes harassment
- is defamatory, abusive, indecent or obscene
- is in breach of confidence, privacy or data protection
- is in breach of any third party intellectual property rights (including copyright)
- is in breach of any other rights or has any fraudulent purpose of effect

You are prohibited from storing, distributing or transmitting or permitting the storage distribution, or transmission (whether intentionally or otherwise) of, any unlawful material through the school IT systems. Examples of unlawful material include but are not restricted to:

- Direct threats of physical harm
- Hard core and child pornography
- Copyrighted, trademarked and other proprietary material used without proper authorisation
- Any other material that may be considered offensive

Examples of S.P.S. systems & storage: -

- Instant messaging or chat
- Local machine hard drive
- Users' home directory o Public directory
- Staff directory
- E-mail

Violations of Systems or Network Security

Any violations of the computer systems or network security are prohibited, and may result in the 'User' facing criminal and civil liability. S.P.S. will investigate such incidents, and will inform and co-operate with the relevant law enforcement agencies if a criminal violation is suspected.

Computer Usage

When using any of the school computer systems and associated equipment, i.e. Computers, Email, Printing, Online Testing etc. the following rules apply: -

- All of the Academy systems are to be used for work that is in connection with your professional role within the Academy
- All IT systems should only be accessed using your own authorised Username and Password
- Your Username and Password should not be shared with anyone else, **students in particular**
  - It is staff's responsibility to ensure that electronic platforms, such as S.P.S logins, CPOMs and email accounts, are correctly logged out when not in use to ensure the safety of both pupils and staff is maintained.
- As regards security, your Passwords should be given the same consideration as your Bank Card number
- Under no circumstances should you use anyone else's Username and Password to access any of the Academy systems
- Should you suspect that anyone has discovered any of your passwords, they should immediately be changed and the details reported to the IT Technician.

  It is recommended that in order to keep your information safe and secure, that you change your passwords regularly (advice on this can be obtained from the IT Technician.
- In order to protect your information, and the school data from unauthorised access, it is expected that when using any of the school systems, you will lock your computer when you are not in attendance.
- All work is to be saved in your Home directory, or in a designated folder on Public or Staff directories, or in the case of Administration Staff, the Common directory
- Although the Academy considers the use of e-mail as an informal method of communication, it is still requisite that the same professional conduct applies to its use, as that of formal communication, i.e. letters, memos etc.
- Staff are responsible for all e-mails that they send, and for any contacts that are made as a result of this, which may result in e-mails being received
- You may not send e-mail to any user who does not wish to receive it, or send emails which could be considered as offensive
- No e-mail bombing or spamming *
- You may not conceal your e-mail address or try to prevent Internet users from responding to messages
- When e-mailing a child you should always copy in your line manager, or another member of staff, to ensure that contact is clear and open
- The posting of anonymous messages and forwarding of emails that are not work related is forbidden
- Use for advertising, gambling, political purposes, personal or financial gain is strictly prohibited
- Accessing, reproducing, sending, posting or distributing anything that is bullying, racist, pornographic, or offensive in nature is strictly prohibited
- Use for cyber bullying, racial harassment or intimidation is strictly forbidden
- The use of Blogs is 'only' allowed on those sites approved by S.P.S.
- Use of chat or instant messaging is permitted but 'only' through those provided by the Academy
- The sending of text or picture messages to mobile phones from the Internet is not allowed unless this is work-related

- You must not give out any of your personal details to children, including mobile phone or home phone numbers, such communication as may be required can be made using a mobile phone provided by school.
- Recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible
- In order to protect yourself, you should never initiate or allow any contact with children through social network sites or other such medium from outside school
- Ensure that personal social networking sites are set at private and children are never listed as approved contacts and use social media in line with the Social Media Policy and Guidelines
- If you do choose to operate a social networking site or blog, any activity that may bring the school into disrepute, will be addressed through disciplinary action
- You should not access any chidlren's social network site
- All software for use on the system must be approved by the IT Team and can only be installed by an IT Technician. Details concerning this can be obtained by contacting the IT Technician.
- Installation of programs and games can only be carried out by a member of the IT Team
- Copying of data that is not for use in connection with your professional role within school (including Images, Videos, Music, or Text) is not allowed
- You may not post or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on any of the school systems, without written consent from the copyright holder. These include but are not restricted to, Music, Videos, Images, or Text
- You are not allowed to delete, move or in any way modify the work of others, without their express permission
- All Internet access must go through Academy systems, which includes the use of personal laptops, tablets etc. Should you require Internet access on a personal device, please contact a member of the IT Team.
- The use of a 'Dongle' to access the Internet from any IT device is strictly prohibited
- Any activity that may cause damage to the computer systems such as, physical abuse, computer hacking or the deployment of a computer virus, or other malicious software is strictly forbidden
- Any misuse or damage to computers should be reported to the IT technician
- Any faulty computer hardware should be reported to the IT technician
- No attempt should be made to repair faulty computer hardware
- It is the user's responsibility to ensure that all removable media, (such as floppy discs, USB pens, CD or DVD ROMs, External Storage Devices etc.) are scanned for viruses before being used on the school IT systems
- All removable data should be handled responsibly and documents containing sensitive information, should only be stored on encrypted and password protected storage media
- All portable IT equipment (such as a laptop or mobile phone) should be stored with appropriate security precautions and such items should not be left in an unattended vehicle

* Mail-bombing is defined as e-mailing copies of a single message to many users, or sending large or multiple files or messages to a single person. Spamming is similar to Mail-bombing but the

message content is aimed at soliciting funds from the recipient, legitimate or illegitimate solicitation.

Violations may include, but are not limited to the following: -

- Unauthorised access to or use of data, software or networks, including any attempt to probe, scan or test for vulnerability of the network
- Unauthorised monitoring of data or traffic on the network, without express permission of the S.P.S. SLT
- Interfering with any user, or the network and deliberate attempts to overload the system
- Irresponsible use of passwords, as these should be changed on a regular basis (and as mentioned above) under no circumstances shared with anyone, staff or child

Filming and Photography

- The taking of photographs or filming of children, is only allowed where permission has been given by receipt of a signed 'Authorisation Form' from a parent or carer, (Office will have details concerning this) and then only if the children concerned give their consent
- Filming and the taking of photographs of children with your own personal mobile phone or camera is forbidden, this should only be undertaken using equipment specifically provided by the Academy for this purpose
- Photographs or videos involving children can only be used in connection with Teaching and Learning within S.P.S. and its partners
  Photographs and videos of childrenshould be edited/ dated/ stored in a Staff shared area wherever possible, and if not possible be clearly marked as to what purpose they are being used, in line with school policy
- Photographs and videos of children should be deleted after use, or if they need to be archived for any purpose, be placed in a shared staff area, in line with school policy

It is expected that all Staff will treat our equipment with respect and not remove or damage any part of the computer systems, i.e. computers, monitors, mice, keyboards, printers, mobile devices etc. S.P.S. reserves the right to examine or delete files that are held on its computer systems, and to monitor Computer usage, Printing, E-mail and Internet activity at any time.

Legal Obligations

The laws of the nation states, regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to online activities. However the practical, legal position regarding Internet usage is often uncertain.

Documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Material must not be accessed from the web, which would be objectionable on the above grounds under the sovereign laws of the countries in which the networks transporting the material are sited, or which would violate the IT Acceptable Usage Policy.

Given the impracticality of accessing the exact legal position with regard to the previous two paragraphs, Skelton Primary School Use Policy governing material that could be objectionable on the above grounds, is grounded in English law.

Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites, i.e. Wikipedia, YouTube, Facebook, Twitter etc.

All Internet usage from our Internet Service Provider is monitored and logged and a log is kept of all sites visited. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and traced to the relevant site and user account. Such an investigation may result in action and possibly criminal investigation.
Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Such files must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

Relevant Legislation

The following are a list of Acts that apply to the use of Northern Grid Network and Services:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
  Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

Disciplinary and Related Action

Failure to comply with any of the rules as stated within the 'IT Agreed Usage Policy for staff' may result in disciplinary action being taken. In the case of any suspected abuse of the school E-mail system, Internet access and General access, the user will have their account suspended pending an investigation into such abuse. The above actions will be mandatory and any other sanctions that the management see fit to impose will also apply. These will be dependent upon the nature and severity of the offence and will not exclude reporting to relevant authorities should there be any criminal implications.

Skelton Primary School wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its users. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Examples: -

- Criminal Acts – for example in relation to child pornography
- Visiting pornographic sites (adult top shelf materials)
- Causing offence to religious groups or racial incitement
- Chat rooms – sexual discourse, arrangements for sexual activity
- Software media counterfeiting or illegitimate distribution of copied software

Decision to Advise the Police for Criminal Investigation

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken.

Where Skelton Primary School are approached by an officer from the Local Authority or any public body asking to provide evidence or monitoring of a suspected site, the following rules will apply.

The Regulation of Investigatory Powers Act 2000 and its Application for Northern Grid

The Home Office states that:

"The Regulation of Investigatory Powers Act 2000 (RIPA) provides for, and regulates the use of, a range of investigative powers, by a variety of public authorities. It updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It also puts other intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act."

Each police force and most local councils including the members of Northern Grid are defined as a Public Authority to which RIPA applies. The forms of surveillance that the police and any council are entitled to authorise are covert directed surveillance and the use of covert human intelligence sources (informants). In any council only officers of the rank of deputy chief officer and above may be designated as Authorising Officers under RIPA. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority from such an Authorising Officer.

RIPA requires that third parties (Northern Grid), that are required to provide information about other people subject to surveillance and investigation, should be approached for that information in a highly controlled manner by means of standard forms published by the Home Office. Northern Grid will require that all such applications for information be made in the appropriate manner.

Disclaimer

SPS will endeavour, wherever possible, to provide a safe and secure environment for its users. However, users must be aware that we cannot guarantee complete safety from inappropriate material. Users must be aware of sites being accessed and report any inappropriate material immediately to the IT Support

Please make sure if you are reporting inappropriate material, you provide the following important information in your email:

- Your Name
- Department
- Basic description of inappropriate site
- Full URL of site copied from the browser address bar (This version of the URL is very important)

Example: - http://www.skeltonprimaryschool.co.uk/ vacancies
Instead of: - www.skeltonprimaryschool.co.uk

Once your email has been received you will receive confirmation of its receipt. You may not always be contacted once the issue has been resolved if it breaches the confidentiality of another member of Staff.

Staff
IT Agreed Usage Policy Consent Form

By signing this consent form you are allowed to access all of the school's IT systems, including the Data Network, Internet, E-mail, Printing and our Frog Virtual Learning Environment. All of our IT systems are here to assist our staff to optimise their use of IT in supporting and delivering Teaching and Learning to the highest standards.

Declaration

I have read the Staff IT Agreed Usage Policy and I agree to use the school's computer systems in accordance with these rules. I understand that if I breach any of these rules, I will be subject to disciplinary action.

Date……………………………………………………………………………………………………..

Print Name……………………………………………………………………………………………

Signed…………………………………………………………………………………………………..

APP E

Social Media/ Networking Policy

Skelton Primary School offers a positive, safe learning environment for its community, in which everyone has equal and individual recognition and respect. We celebrate success and are committed to the continuous improvement and fulfilment of potential in every child.
We encourage increasing independence and self-discipline amongst the pupils. Everyone within the school has an important role to play in sharing responsibility for the development of positive behavior and attitudes.

1. Aims:

At Skelton, we have high aspirations and ambitions for our children and we believe that no child should be left behind. We strongly believe that it is not about where you come from but your passion and thirst for knowledge, and your dedication and commitment to learning; your 'UMPHHHH' that make the difference between success and failure, and we are determined to ensure that our children are given every chance to realize their full potential. This policy recognizes that new technology are an integral and growing part of everyday life and make an important contribution to teaching and learning opportunities. However, rapid evaluation of social networking technologies requires a robust policy framework and this policy aims to:

- Assist staff working with children to work safely and responsibly with the internet and other communications technologies and to monitor their own standards and practice.
- Give a clear message that unlawful and unsafe behavior is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken.
- Set a clear expectations of behavior and/or codes of practice relevant to social networking for educational, personal and recreational use.
- Support safer working practice.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Prevent adults abusing or misusing their position of trust.

This policy applies to all staff who work in the school whether paid or unpaid. This includes members of the Governing Body, where Parent, Community or Local Authority Governors.

2. Background

Social networking and social media are communication tools based on websites or networks which allows you to share information or other material about yourself and your interests with groups of other people. These groups of people could be:

- People who are known to you (friends or colleagues)
- People you don't know who share common interests.
- Anyone who could find your comments through search engines

3. Context

This policy is concerned mainly about two types of social media activity:

- Your personal activity done for your friends and contacts, but not under or in the name of Skelton Primary School.
- Activity carried out in the name of Skelton Primary School, such as school blog, twitter, Facebook that represents the school, or that appears to represent the official views of the

school.

This policy is not about stopping you using or accessing such groups, but aims to ensure that your use of social media that does not harm the reputation of the school or school staff and ensure the interests of the children are supported.

4. Key Principles

The principles that underpin this policy are:

- Adults who work with pupils are responsible for their own actions and behaviour and must avoid any conduct which would lead any responsible person to question their motivation or intensions.
- Adults in the school must work and be seen to work, in an open and transparent way.
- Adults in the school must continually monitor and review their own practice in terms of the continually evolving world of social media and ensure that they consistently follow the guidance in this document.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things in social media that they have later regretted, because that information has harmed or put at risk themselves or others. This includes:

- Accidently posting personal or embarrassing information about themselves or others in a public forum or beyond the group information was originally intended for.
- Sharing information about yourself or others with people you don't know that could be used by someone to commit fraud or misrepresent the views of yourself or others (such as identity theft)
- Breaching privacy or child protection laws and regulations or workplace policies by posting information about your work or the children and adults that you work with.
- You or others receiving negative publicity, harassment, inappropriate contact or threats as a result of your views, beliefs or comments.

This has led to people facing disciplinary actions, losing their jobs, being prosecuted or even imprisoned. This policy and guidance will make sure sites such as Facebook, Twitter, etc. and all other current and emerging technologies are a safe place.

Safer Networking Practice applies to current social networking sites such as Facebook, Twitter etc and all other current emerging technologies.

My Safer Social Networking Practice is broken down into:

- Things you must not do, because they are illegal, contrary to regulations or against school policy (such as professional boundaries)
- Things you should do to avoid risk to yourself or others
- Good practice things you should do to reduce the risk that information you put on social networking sites or media cannot later be used against you.

All staff and volunteers must adhere to and apply the principles of this document in all aspects of work. Failure to do so may lead to action being taken inder the disciplinary procedure.

5. Monitoring

Social Network "Must Nots"

- Staff or volunteers must not make comments on behalf of the school or claim to represent the views of the school, unless they have explicit permission to do so.
- Staff and volunteers should never make a 'friend' of a pupil at the school where they are working on their social networking page and seek advice or the Headteacher, Deputy Head or IT leader before becoming 'friends' with ex –pupils.
- Staff and volunteers should not make a 'friend' of a parent/carer of a pupil at the school , and should seek advice of the Headteacher, Deputy Head or IT leader before becoming 'friends' with parents/carer of ex –pupils.
- Staff and volunteers should never use or access social networking pages of pupils.
- Staff and volunteers must not request, or respond to , any personal information from a pupil.
- Staff and volunteers should never post confidential information about themselves, the school, the governing body, the local authority, their colleagues, pupils. IF they are posting in an 'official' capacity they should not post confident information about members of the public.
- Staff and volunteers should not make allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or other school, or local authority. Doing so may results in disciplinary action being taken against them. If they have concerns about practices within school or actions or pupils or parents, they must act in accordance with the school Whistle-Blowing Policy.
- E-mail or text communications between staff member/volunteer and a pupil outside must not take place outside the agreed protocols (Acceptable use policy)

Social Networking "Shoulds"

- All adults, particularly those new to the school, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.
- In their own interests, adults with the school setting need to aware of the dangers of putting their personal information onto social networking sites such as addresses, home or mobile numbers. This will avoid the potential for pupils or their families or friends having access to staff outside the school environment. It also reduces the potential for identity theft by third parties.
- Some social networking site and other web based sites have fields in the user profile for job title etc. As an employee or volunteer of the school and particularly if you are a teacher

or teaching assistant, you should not out on any information onto the site that could identify either your profession or school where you work. In some circumstances this could damage the reputation of the school and the profession. If it is a work-based site where you are required to provide this information, you must obtain permission of the Headteacher or Deputy beforehand.

- Staff and volunteers should keep their personal phone number, work login or password and professional email addresses private and secure. Where there is a need to contact pupils or parents the school email address and/or telephone should be used. If, with permission, telephone call are made from a personal phone (landline/mobile) the telephone number the call is being made from must be withheld when making call by prefixing the dialed number 141.
- Staff and volunteers should ensure that all communications are transparent and open to scrutiny. They should be circumspect in their communities with pupils in order to avoid any possible misinterpretation of their motives or any behavior which could possibly be construed as 'grooming' in context of sexual offending.
- E-mail or text communication between members of staff and volunteers and a pupil should only take place within the agreed protocols and for email within the confines of the Acceptable Use Policy.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will easily be recognized and should be openly acknowledged with the Headteacher where there may be implications for the adult and the position within the school setting

6. Reporting/Posting

Posting on behalf of the school
Staff members are not permitted to post on behalf of school without specific permission, which will apply to specific sites

Social Networking Good Practice
Staff and volunteers must understand who is allowed to view the content of their page of any sites they use and how to restrict access to certain groups of people.

- On FACEBOOK, they should understand whether the posts they make are public (which means that anyone can see them), visible to Friends (which means only people on their friends list can see them) or visible to friends of friends (which means posts are visible to all their friends of their friends which could be hundreds even thousands of people)
- On TWITTER and LINKEDIN, all posts, unless they are direct messages to another user, are visible to everyone (the whole world)
- If you are unsure of who can see your posts on other sites, you could always assume that the information is publically available to all and could be found by people doing a search on Google,

for example.

Before posting, staff and volunteers should ask themselves the following questions:

1. Do you want the whole world to see? Even if you restrict your own visibility settings, these can be overridden by the setting of other, or people can copy and paste information into other public places.
2. Do you want the post to be forever? Once you have posted something, it is almost impossible to delete it again from the internet, even if you delete it from the sites. There are sites that archives all Twitter posts, for example, so even if you delete a post it can still be found.
3. What information is taken out of context? It is very easy for others to take what is posted, alter it, and re-post it elsewhere. It is also possible that your hard work, posted online , maybe used inappropriately by others.
4. Could the information out you or others in danger? What you post could tell others that your house is empty or that pupils in your class are in a school trip, which could have implications for a looked after child.
5. Are you violating any laws? The information could be breach of copyright, or specific legislation relating to privacy of vulnerable groups, for example. What you post could be illegal in other countries, which could have serious implications if you were to visit there, Are you making claims that could be taken as facts when they are not? This could lead to you being accused of slander.
6. Is your message clear? Could you unintentionally break cultural norms or putting out something unintentionally offensive? Is it clear whether or not you are posting in an official capacity?
7. Could the actions of your social networking friends reflect on you? Could your friends or friends ‘tag’ you in a photograph or link you inappropriate activities through their own posts? Choose your friends carefully.

Access to inappropriate Images

Although this is covered in the Acceptable Use Policy, there is an overlap with social networking, so these principles are re-stated for the purpose of clarity:

- There are no circumstances that justify adults possessing images of children. Staff and volunteers who access and/or possess links to such material or websites will be viewed as a significant and potential threat to children. This will lead to criminal investigations and disciplinary action. Where indecent images of children are found, the Headteacher will be informed immediately.
- Adults must not use equipment belonging to school to access any adult pornography; neither should personal equipment containing images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.
- Adults should ensure that all pupils are not exposed to any appropriate images or web links. The school endeavors to ensure that internet equipment used by pupils has appropriate controls with regards access. Eg personal password should be kept confidential. Any potential issues identified must be reported to the IT lead or IT technician, if this is a significant issue report to the Headteacher.
- Where other unsuitable material is found, which may not be illegal but which could or does raise concerns about a member of staff, high level advice should be sought before any

investigation is conducted.

- Staff and volunteers should be aware that they could be drawn into an investigation of child pornography or obscene images if they are linked to someone under investigation through social media networking sites. They should inform the Headteacher immediately if they are contacted by the police or other investigators.

Cyberbullying
Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control them.'
If cyberbullying does take place, employees should keep records of abuse, text, emails, websites or instant message and should not delete text or emails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.
Employees are encouraged to report any and all incidents of cyberbully to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police. Employees may wish to seek the support of their union or professional association representatives.

Pupil use of social media

Students' use of personal social networking should avoid: -
□ Use of any social networking if under the age of 13
□ Use of social networking sites on the school premises, including using mobile devices independent of the Academy's computer network
□ Attempting to access or view private staff social network accounts
□ Sending any social media message that is regarded as offensive, harassment or of a bullying nature whether in school or at home.

Staff are to act upon any social media post that they become aware of which could be regarded as 'peer on peer abuse' as Keeping Children Safe in Education 2020 states:

safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but may not be limited to, bullying (including cyberbullying), gender based violence/sexual assaults and sexting. Staff should be clear as to the school or college's policy and procedures with regards to peer on peer abuse.

Pupils who do not adhere to the school's online safety and social media policies may find themselves subject to sanctions within school, even if the postings occurred outside school hours. (See online safety policy point 2.2)