E-Safety Policy

Name of Unit/Premises/Centre/School	The Toynbee School
Date of Policy Issue/Review	November 2021/ November 2022 (Annually)
Name of Responsible Manager/Headteacher	Mr M. Longden (Headteacher)
Governors' Sub-Committee	Teaching and Learning

1. Overview

1.1 This e-Safety policy recognises the commitment of our school to e-Safety and acknowledges its part in the school's overall Safeguarding policies and procedures (this includes PREVENT). It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

1.2 Our expectations for responsible and appropriate conduct are formalized in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

1.3 As part of our commitment to e-Safety we also recognize our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

2. Scope of Policy

This policy applies to the whole school community including the senior leadership team, (SLT) school board of governors, all staff employed directly or indirectly by the school, visitors and all pupils.

2.1 Our expectations for responsible and appropriate conduct are formalized in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

2.2 The senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safety within school will be reflected within this policy.

2.3 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 is pertinent to incidents of cyberbullying, or other e-Safety-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

2.4 The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the head teacher believes it contains any material that could be used to bully, harass or put children's safety & wellbeing at risk.

2.5 This policy incorporates and is guided by the 'Revised Guidance for Safer Working Practices for Adults who work with Children & Young People in Education,' July 2015.

2.6 The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies & overarching Safeguarding Policy. The school will, where known, inform parents and carers of incidents of inappropriate e-Safety behaviour that take place out of school.

3. Responsibilities of Governing Body

3.1 Read, understand, contribute to and help promote the school's e-Safety policies and guidance as part of the school's overarching Safeguarding procedures.

3.2 Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safety awareness.

3.3 To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data. Ensure appropriate funding and resources are available for the school to implement their e-Safety strategy

4. Implementation of the policy

4.1 The person in school taking on the role of e-Safety lead is Matthew Longden and Paul Lawrence (DSLs).

4.2 The Governor with an overview of e-Safety matters is Garry Moore (Chair of Governors).

4.3 The following groups were consulted during the creation of this e-Safety policy: ICT Dept, Network Support Dept, Senior Leadership Team & Governors.

4.3.1 The Senior Leadership Team will ensure that all members of school staff are aware of the contents of the school e-Safety policy and the use of any new technology within school.

4.3.2 The Senior Leadership Team will ensure that all school staff complete the required e-Safety training.

4.3.3 All staff, pupils, occasional and external users of our school ICT equipment will sign the relevant Acceptable Use Policies.

4.3.4 All amendments will be published and awareness sessions will be held for all members of the school community.

4.3.5 E-Safety will be taught as part of the curriculum in an age-appropriate way to all pupils.

4.3.6 E-Safety posters and information will be prominently displayed around the school.

4.4 The following national guidance is acknowledged and included as part of our e-Safety policy: **Revised Guidance for Safer Working Practices for Adults who work with Children and Young People in Education** produced by DCSF in July 2015 and is still current. This guidance provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. We acknowledge the guidance given in the following sections of the DCSF document and accept this as part of our policy. (See Appendix 1)

5. Responsibilities of the School Community

5.1 We believe that e-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring 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.

6. The senior leadership team accepts the following responsibilities:

6.1 The Headteacher will take ultimate responsibility for the e-Safety of the school community.

6.2 Identify a person (the e-Safety lead) to take day to day responsibility for e-Safety; provide them with training; monitor and support them in their work.

6.3 Ensure adequate technical support is in place to maintain a secure ICT system.

6.4 Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets.

6.5 Ensure liaison with the Governors.

6.6 Develop and promote an e-Safety culture within the school community.

6.7 Ensure that all staff, pupils and other users agree to the Acceptable Use Policy (AUP) and that new staff have e-Safety included as part of their induction procedures.

6.8 Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to e-Safety.

6.9 Receive and regularly review e-Safety incident logs; ensure that the correct procedures are followed should an e-Safety incident occur in school and review incidents to see if further action is required (some e-safety incidents will of necessity be recorded in the Child Protection log).

6.10 Promote an awareness and commitment to e-Safety throughout the school.

6.11 Be the first point of contact in school on all e-Safety matters.

6.12 Take day to day responsibility for e-Safety within the school.

6.13 Create and maintain e-Safety policies and procedures.

6.14 Develop an understanding of current e-Safety issues, guidance and appropriate legislation.

6.15 Ensure delivery of an appropriate level of training in e-Safety issues.

6.16 Ensure that e-Safety education is embedded across the curriculum.

6.17 Ensure that e-Safety is promoted to parents and carers.

6.18 Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy (AUP).

6.19 Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate.

6.20 Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an e-Safety incident.

6.21 Ensure that Good Practice Guides for Safety are displayed in ICT classrooms and around the school.

6.22 To promote the positive use of modern technologies and the internet.

6.23 To ensure that the school e-Safety policy and Acceptable Use Policies are reviewed at prearranged time intervals.

7. Responsibilities of all Staff

7.1 Read, understand and help promote the school's e-Safety policies and guidance.

7.2 Read, understand and adhere to the staff AUP.

7.3 Take responsibility for ensuring the safety of sensitive school data and information.

7.4 Develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to their work.

7.5 Maintain a professional level of conduct in their personal use of technology at all times.

7.6 Ensure that all digital communication with pupils is on a professional level and only through school based systems, **NEVER** through personal email, text, mobile phone social network or other online medium.

7.7 Embed e-Safety messages in learning activities where appropriate.

7.8 Supervise pupils carefully when engaged in learning activities involving technology.

7.9 Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.

7.10 Report all e-Safety incidents which occur in the appropriate log and/or to their line manager.

7.11 Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

8. Additional Responsibilities of Technical Staff

8.1 Support the school in providing a safe technical infrastructure to support learning and teaching.

8.2 Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date.

8.3 Ensure that provision exists for misuse detection and malicious attack.

8.4 At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed.

8.5 Report any e-Safety-related issues that come to their attention to the e-Safety lead and/or senior leadership team.

8.6 Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management.

8.7 Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment.

8.8 Liaise with the Local Authority and others on e-Safety issues.

8.9 Document all technical procedures and review them for accuracy at appropriate intervals.

8.10 Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

9. Responsibilities of pupils

9.1 Read, understand and adhere to the Pupil AUP and follow all safe practice guidance.

9.2 Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school.

9.3 Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

9.4 Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening.

9.5 Report all e-safety incidents to appropriate members of staff.

9.6 Discuss e-safety issues with family and friends in an open and honest way.

9.7 To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices.

9.8 To know, understand and follow school policies regarding Cyberbullying and keeping themselves safe on-line.

10. Responsibilities of Parents and Carers

10.1 Help and support the school in promoting e-Safety.

10.2 Read, understand and promote the Pupil AUP with their children.

10.3 Discuss e-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.

10.4 Consult with the school if they have any concerns about their child's use of technology.

10.5 To agree to, and sign the Home School Agreement which clearly sets out the use of photographic and video images of pupils.

11. Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club

11.1 Take responsibility for liaising with the school on appropriate use of the school's IT equipment and internet, including providing an appropriate level of supervision where required.

11.2 Ensure that participants follow agreed Acceptable Use Procedures.

12. School Acceptable Use Policies (AUPs)

12.1 Toynbee School has a two AUPs for different users. These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate AUP.

13. Teaching & Learning

13.1 We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

13.2 We will deliver a planned and progressive scheme of work to teach e-Safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. We believe that learning about e-Safety should be embedded across the curriculum and also taught in specific lessons such as in ICT, tutor time, assemblies and PSHE curriculum.

13.3 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. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

13.4 We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology in lessons.

13.5 We will remind pupils about the responsibilities to which they have agreed through the AUP.

13.6 Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

14. How parents and carers will be involved

14.1 We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

14.2 To achieve this we will offer opportunities for finding out more information through Parent Forums, Headteacher's Newsletter. School Comms and signposting to e-safety articles on our website.

15. Managing and safeguarding IT systems

15.1 The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

15.2 Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

15.3 All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. nominated and members of technical support.

15.4 The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals e.g. a member of technical support.

15.5 We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

16. Filtering Internet access

16.1 Web filtering of internet content is provided by Hampshire LA as well as additional local filtering. This ensures that all reasonable precautions are taken to prevent access to illegal content. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.

16.2 All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

16.3 Teachers are encouraged to check out websites they wish to use prior to lessons for the suitability of content.

16.4 Notices are posted around school as a reminder of how to seek help.

17. Access to school systems

17.1 The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

17.2 All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

17.3 Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

17.4 Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

17.5 Remote access to school systems is covered by specific agreements and is never allowed to unauthorized third party users.

18. Passwords

18.1 We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).

18.2 We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.

18.3 All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school.

18.4 All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

18.5 The school maintains a log of all accesses by users and of their activities while using the system in order to track any e-Safety incidents via Securus.

19. Using the Internet

19.1 We provide the internet to:

19.1.1 Support curriculum development in all subjects
19.1.2 Support the professional work of staff as an essential professional tool
19.1.3 Enhance the school's management information and business administration systems
19.1.4 Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

19.2 Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

19.3 All users of the school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

19.4 Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

20. Using email

20.1 Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

20.2 Use of the school e-mail system is monitored and checked.

20.3 It is the personal responsibility of the email account holder to keep their password secure.

20.4 As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

20.5 School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils on the out-of-school times when emails may be answered.

20.6 Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

20.7 Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

21. Publishing content online

21.1 School website:

21.1.1 The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

21.1.2 The point of contact on the web site is the school address, e-mail and telephone number.

21.1.3 Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

21.2 Creating online content as part of the curriculum:

21.2.1 As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school where possible. Pupils will only be allowed to post or create content on sites

21.2.2 where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

21.2.3 We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

21.3 Online material published outside the school:

21.3.1 Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

21.3.2 Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

22. Using images, video and sound

22.1 We recognize that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

22.2 Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

22.3 We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

22.4 We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

22.5 For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

22.6 We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

23. Using mobile phones

23.1 During lesson time we expect all mobile phones belonging to staff & pupils to be switched off unless there is a specific agreement for this not to be the case.

23.2 Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. (In an emergency, where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.)

23.3 Unauthorized or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member we do not consider it a defence that the activity took place outside school hours. Appropriate disciplinary or legal action will be taken.

23.4 The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

23.5 We make it clear to staff, pupils and parents that the Headteacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

24. Using mobile devices

24.1 We recognize that the multimedia and communication facilities provided by mobile devices such iPad, iPod, tablet, netbook and Smart phones, can provide beneficial opportunities for pupils. However their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

24.2 Pupils are taught to use them responsibly.

25. Using other technologies

25.1 As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an e-Safety point of view.

25.2 We will regularly review the e-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

25.3 Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

26. Protecting school data and information

26.1 Toynbee School recognizes their obligation to safeguard staff and pupils' sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

26.2 The school is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

26.3 Pupils are taught about the need to protect their own personal data as part of their e-Safety awareness and the risks resulting from giving this away to third parties.

26.4 Staff are made fully aware of the contents of the MOPP (Manual of Personnel Practice) via the annually updated Staff Planner, which should be referenced alongside this policy.

26.5 Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following :

- 26.5.1 All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- 26.5.2 Staff are provided with appropriate levels of access to the school management information system holding pupil data. Passwords are not shared and administrator passwords are kept securely
- 26.5.3 Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- 26.5.4 All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
- 26.5.5
- 26.5.6 When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- 26.5.7 Remote access to computers is by authorized personnel only

26.5.8 We have full back up and recovery procedures in place for school data

26.5.9 Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example, Governors or School Improvement Officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

27. Management of assets

27.1 Details of all school-owned hardware and software are recorded in an inventory.

27.2 All redundant IT equipment is 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.

27.3 Disposal of any ICT equipment will conform to The Producer Responsibility Regulations, specifically 'The Waste Electrical and Electronic Equipment (WEEE) Jan 2015. Further information can be found on their website https://www.gov.uk/government/collections/producer-responsibility-regulations#waste-electrical-and-electronic-equipment-(weee)

28. Dealing with e-Safety incidents

28.1 All e-Safety incidents are recorded on SIMS or the CPOMS (Child Protection Online Monitoring and Safeguarding system) which is regularly reviewed.

28.2 Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

28.3 In situations where a member of staff is made aware of a serious e-Safety incident, concerning pupils or staff, they will inform the e-Safety Lead, their line manager or head teacher who will then respond in the most appropriate manner.

28.4 Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

28.5 Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's e-Safety Lead and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

28.6 The School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

29. Dealing with a Child Protection issue arising from the use of technology:

29.1 If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the safeguarding policy will be followed.

30. Dealing with complaints and breaches of conduct by pupils:

30.1 Any complaints or breaches of conduct will be dealt with promptly

30.2 Responsibility for handling serious incidents will be given to a senior member of staff such as a Progress Director or the Senior Leadership Team.

30.3 Parents and the pupil will work in partnership with staff to resolve any issues arising

30.4 Restorative practice will be used to support the victims

30.5 There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

31. The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):

31.1 accessing inappropriate or illegal content deliberately

31.2 deliberately accessing, downloading and/or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

31.3 continuing to send or post material regarded as harassment, or of a bullying nature after being warned

31.4 staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

31.5 The following activities are likely to result in disciplinary action:

31.5.1 any online activity by a member of the school community which is likely to adversely impact on the reputation of the school

31.5.2 accessing inappropriate or illegal content accidentally and failing to report this

31.5.3 inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons

31.5.4 sharing files which are not legitimately obtained e.g. music files from a file sharing site

31.5.5 using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute

31.5.6 attempting to circumvent school filtering, monitoring or other security systems

31.5.7 circulation of commercial, advertising or 'chain' emails or messages

31.5.8 revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

31.5.9 using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)

31.5.10 transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988

31.6 The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve:

31.6.1 accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time

31.6.2 accessing non-educational websites (e.g. gaming or shopping websites) during lesson time

31.6.3 sharing a username and password with others or allowing another person to log in using your account

31.6.4 accessing school ICT systems with someone else's username and password

31.6.5 deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

31.6.6 Guidance for staff on the consequences of the misuse of electronic equipment can be found in the document 'Hampshire MOPP'.

32. References to related documents:

32.1 Acceptable Use Policies (Pupils, Staff, Visitors)

32.2 Letter for Parents explaining the AUP and agreement to sign

32.3 Hampshire MOPP (Hampshire Manual of Personnel Practice)

32.4 Toynbee School's PREVENT Policy

Appendix 1

Revised Guidance for safer Working Practices for Adults who work with Children & Young People in Education DCSF July 2015

Section 12 Communication with children (including the use of technology)

In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. E-safety risks are posed more by behaviours and values than the technology itself.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.)

Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'

Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable.

This means that adults should:

- *not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work*
- *use only equipment and Internet services provided by the school or setting*
- *follow their school / setting's Acceptable Use policy*
- *ensure that their use of technologies could not bring their employer into disrepute*

Staff should, in any communication with children, also follow the guidance in section 7 'Standards of Behaviour'.

Staff should adhere to their establishment's policies, including those with regard to communication with parents and carers and the information they share when using the internet.

Section 24. Photography, videos and other images

Many educational activities involve recording images. These may be undertaken for displays, publicity, to celebrate achievement and to provide records of evidence of the activity. Under no circumstances should staff be expected or allowed to use their personal equipment to take images of pupils at or on behalf of the school or setting.

All settings should have arrangements with regard to the taking and use of images, which is linked to their safeguarding and child protection policy. This should cover the wide range of devices which can be used for taking/recording images e.g. cameras, mobile-phones, smart phones, tablets, web-cams etc. and arrangements for the use of these by both staff, parents and visitors.

Whilst images are regularly used for very positive purposes adults need to be aware of the potential for these to be taken and/or misused or manipulated for pornographic or 'grooming' purposes. Particular regard needs to be given when images are taken of young or vulnerable children who may be unable to question why or how the activities are taking place.

Pupils who have been previously abused in a manner that involved images may feel particularly threatened by the use of photography, filming etc. Staff should remain sensitive to any pupil who appears uncomfortable and should recognise the potential for misinterpretation.
Making and using images of pupils will require the age appropriate consent of the individual concerned and their parents/carers. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the setting have access.

- *This means that staff should:*
- *adhere to their establishment's policy*
- *only publish images of pupils where they and their parent/carer have given explicit written consent to do so*
- *only take images where the pupil is happy for them to do so*
- *only retain images when there is a clear and agreed purpose for doing so*
- *store images in an appropriate secure place in the school or setting*
- *ensure that a senior member of staff is aware that the photography/image equipment is being used and for what purpose*
- *be able to justify images of pupils in their possession*
- *avoid making images in one to one situations*

- *This means that adults should not:*
- *take images of pupils for their personal use*
- *display or distribute images of pupils unless they are sure that they have parental consent to do so (and, where appropriate, consent from the child)*
- *take images of children using personal equipment*

For the protection of children, it is recommended that when using images for publicity purposes that the following guidance should be followed:

- if the image is used, avoid naming the child, (or, as a minimum, use first names rather than surnames)
- if the child is named, avoid using their image
- schools and settings should establish whether the image will be retained for further use, where and for how long
- images should be securely stored and used only by those authorised to do so.

Section 25. Exposure to inappropriate images

Staff should take extreme care to ensure that children and young people are not exposed, through any medium, to inappropriate or indecent images.

There are no circumstances that will justify adults: making, downloading, possessing or distributing indecent images or pseudo-images of children (child abuse images). Accessing these images, whether using the setting's or personal equipment, on or off the premises, or making, storing or disseminating such material is illegal.
If indecent images of children are discovered at the establishment or on the school or setting's equipment an immediate referral should be made to the Designated Officer, (DO) and the police contacted if relevant. The images/equipment should be secured and there should be no attempt to view or delete the images as this could jeopardise necessary criminal action. If the images are of children known to the school, a referral should also be made to children's social care in line with local arrangements.

- *take images of children in a state of undress or semi-undress*
- *take images of children which could be considered as indecent or sexual*

This means that staff should:
 abide by the establishment's acceptable use and e-safety policies
 ensure that children cannot be exposed to indecent or inappropriate images
 ensure that any films or material shown to children are age appropriate

Under no circumstances should any adult use school or setting equipment to access pornography. Personal equipment containing pornography or links to it should never be brought into or used in the workplace. This will raise serious concerns about the suitability of the adult to continue working with children and young people.

Staff should keep their passwords confidential and not allow unauthorised access to equipment. In the event of any indecent images of children or unsuitable material being discovered on a device the equipment should not be tampered with in any way. It should be secured and isolated from the network, and the DO contacted without delay. Adults should not attempt to investigate the matter or evaluate the material themselves as this may lead to a contamination of evidence and a possibility they will be at risk of prosecution themselves.

This means that staff should:
- *abide by the establishment's acceptable use and e-safety policies*
- *ensure that children cannot be exposed to indecent or inappropriate images*
- *ensure that any films or material shown to children are age appropriate*