Exeter House School Online Safety Policy

March 2017

This document has been written with the following key principles in mind;

• All individuals are protected from inappropriate material, bullying and harassment

• Users have access to resources to support learning and teaching

• Users should be given clear boundaries on responsible and professional use

**Disclaimer**

Exeter House School has made every effort to ensure that the information is accurate and up to date. If errors are brought to our attention we will correct them as soon as is practically possible. However, Exeter House School and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.

# 1. Leadership and Management

# 1.1 Developing a policy

The school e-safety policy will feature as part of the review process within the School Development Plan. It relates to other policies including those for behaviour, for personal, social and health education (PSHE), for anti- bullying, child protection, Staff Code of Conduct for Safer Working Practice, and for citizenship.

Our e-safety policy has been written by the school, building on the Wiltshire e-safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Created by: Andrew Walker Date: March 2017

 Approved:

 *Review Date:* March 2018

# 1.2 Authorised Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission should be sought at least at the start of each Key Stage.

* *The school receives Internet Service Provision (ISP) from School Care and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.*
* *The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil’s access is withdrawn.*
* *All users of the school’s IT systems will sign the Responsible Use Policy and read guidance for sound, image and video for publication online. (See The Wiltshire E Safety Toolkit).*
* *Secondary students must apply for Internet access individually by agreeing to abide by the Responsible Use Policy statement that is signed in conjunction with their parents (See the Wiltshire E Safety Toolkit).*
* *At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.*
* *Parents will be informed that pupils will be provided with supervised Internet access (This will be done when pupils join Exeter House School and annually when parents are asked to update their child’s data sheet.*

# *1.3 Filtering and Monitoring*

*Despite careful design, filtering systems cannot be comp*l*et*ely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil’s age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

* *A log of all staff with unfiltered access to the Internet will be kept and regularly reviewed.*
* *The Network Managers will review the popular permitted and banned sites accessed by the school each term.*
* *The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.*
* *If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the Network Manager.*
* *Website logs will be regularly sampled and monitored. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Network Managers will bring Filtering Logs will be brought to E Safety / Data Security team meetings for review.*
* *Any material that the school believes is illegal must be referred to the Internet Watch Foundation and/or police and/or DOA*
* *All filtering change requests to be submitted in writing to the to E Safety / Data Security team meetings for review.*

**1.4 Risk Assessment**

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

* *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.*
* *Methods to identify, assess and minimise risks will be reviewed regularly.*
* *The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.*
* *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.*

# 2. Teaching and Learning

**2.1 The Curriculum**

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e‑mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

* *Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.*
* *The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school’s management information and business administration systems.*
* *Internet access is an entitlement for students who show a responsible and mature approach to its use.*
* *The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.*
* *Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.*

**2.2 Enhancing Teaching and Learning**

Benefits of using the Internet in education include:

* *Access to worldwide educational resources including museums and art galleries;*
* *Inclusion in the National Education Network which connects all UK schools;*
* *Educational and cultural exchanges between pupils worldwide;*
* *Vocational, social and leisure use in libraries, clubs and at home;*
* *Access to experts in many fields for pupils and staff;*
* *Professional development for staff through access to national developments,*
* *Educational materials and effective curriculum practice;*
* *Collaboration across networks of schools, support services and professional associations;*
* *Improved access to technical support including remote management of networks and automatic system updates;*
* *Access to learning wherever and whenever convenient.*

**2.3 Evaluating Content**

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

* *Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy This will be done taking into consideration the understanding of our students.*
* *Pupils will use age-appropriate tools to research Internet content.*
* *The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.*
* *If staff or pupils discover unsuitable sites, the URL (address) and content should be reported to their ISP/ School Care, via the school’s Network Managers.*
* *Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*

Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

**3. Communication and Content**

**3.1 Website Content**

Many schools have excellent websites that inspire pupils to publish work of a high standard. Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school’s requirements for accuracy and good presentation.

* *The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils’ personal information will not be published.*
* *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individual pupils to be clearly identified.*
* *Staff members will only be named on the website or associated with a photo/video if they have given their consent. (Exeter House will only seek consent from the Teaching Staff)*
* *The nature of all items uploaded will not include content that allows the pupils to be identified. Network Managers will inspect the website each week to identify if the aggregation of several separate pieces of information could place a pupil at risk*
* *The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.*

*The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.*

**3.2 Learning Platforms**

An effective learning platform (LP) or virtual learning environment (VLE) can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration.

* *All users will be required to use an age appropriate password to access the relevant content of the LP, which they must not share with others*
* *SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.*
* *Pupils/staff will be advised about acceptable conduct and use when using the LP.*
* *Only members of the current pupil, parent/carers and staff community will have access to the LP.*
* *All users will be mindful of individual and intellectual property and will upload only appropriate content to the LP.*
* *When a user leaves the school their account or rights to relevant content areas will be disabled or transferred to their new establishment.*

# 3.3 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

Schools will need to determine the best approach for their circumstances, based upon pupil age and curriculum requirements. The use of email identities such as john.smith@school.wilts.sch.uk generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people.

* *Pupils may only use approved e-mail accounts on the school system.*
* *Pupils must immediately tell a responsible adult if they receive offensive e-mail.*
* *Staff must use official school provided email accounts for all professional communications.*
* *Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school RUP and will be dealt with accordingly.*
* *E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper.*

# 3.4 On-line communications and Social Media.

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

The school will organize regular training so that all staff are aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

* *Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.*
* *Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.*
* *Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.*
* *Staff official blogs or wikis should be password protected and only run with approval from the SLT.*
* *Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.*
* *Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.*
* *No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.*
* *A member of the school SLT will make an announcement at school events to which parents are invited reminding them that photographs should not be shared on social media.*
* *Concerns regarding students’ use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students’ underage use of sites.*
* *Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.*
* *In line with, ‘Guidance for Safer Working Practice for Adults who Work with Children and Young People’ it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.*

# 3.5 Mobile Devices (Including BYOD)

**Mobile devices** refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet access all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for schools to achieve. Due to the widespread use of mobile devices it is essential that schools take steps to ensure that these devices, both personally and school owned, are used responsibly.

Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

* All individuals are protected from inappropriate material, bullying and harassment
* users have access to resources to support learning and teaching
* users should be given clear boundaries on responsible and professional use

 The following points, whilst not exhaustive, have been provided to support schools in creating effective policies.

* *Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.*
* *School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation*.
* *Sending abusive or inappropriate messages or content is forbidden by any user within the school community.*
* *School or County or approved privately owned Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum based activity. These devices will have profiles and device management software installed by the school. Use of mobile devices in the school is conditional upon acceptance of these. This applies to all mobile devices used in school, regardless of their ownership.*
* *Mobile devices are not permitted to be used in certain areas or situations within the school site such as changing rooms or toilets, situations of emotional distress, challenging behaviour etc.*
* *Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e mail, phone, social media) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP*
* *Staff needing to contact a pupil or person under the age of 18 should do so via the pupil’s school (or college or other institution) account (telephone, e mail or social media etc.) and not to a personal account held by the pupil.*
* *Staff are provided with school equipment for taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for emergency purposes and when doing so, should ensure they comply with the schools Responsible Use Agreement.*
* *For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user’s device.*
* *The school will take steps to monitor responsible use in accordance with the Responsible Use Policy*

# 3.6 Video Conferencing

Video conferencing (including FaceTime, Skype and Lync) enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many potential benefits in education and where possible should take place using the school’s wireless system.

* *Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.*
* *All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*
* *Pupils will ask permission from a teacher before making or answering a video conference call.*
* *Video conferencing will be supervised appropriately for the pupils’ age and ability.*

**3.7 Emerging Technologies**

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment should be completed on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

* *Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.*

**3.8 Cyber Bullying**

**Cyber bullying** can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school’s behaviour, anti-bullying, or child protection policies, which should include:

* *Clear procedures in set out to investigate incidents or allegations of cyber bullying. See schools’ Anti Bullying Policy*
* *Clear procedures in place to support anyone in the school community affected by cyber bullying.*

 *All incidents of cyber bullying reported to the school will be recorded.*

* *The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.*
* *Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school’s e-Safety ethos.*
* *The school is committed to regarding e-safety as a wider community issue and will deal rigorously with out of school e-safety incidents that relate to members of the school community.*

**3.9 Data Protection**

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The GDPR give individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Data Protection Act; this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the GDPR see <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>

* *Personal data will be recorded, processed, transferred and made available according to the GDPR 2017.*

# 4 Implementation

**4.1 Policy in Practice-Pupils**

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school’s e-safety teaching and awareness-raising it is important to discuss the key features with pupils / students as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

* *All users will be informed that network and Internet use will be monitored.*
* *Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.*
* *Online Safety teaching will be included in the PSHE, Citizenship and/or ICT and cover safe use at school and home.*
* *Online Safety rules or copies of the student Responsible Use Policy will be on display in all rooms with Internet access.*
* *Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.*
	1. **Policy in Practice- Staff**

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies with a member of the eSafety Team.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

* *The Online Safety Policy will be provided to and discussed with all members of staff and RUP signed for compliance.*
* *Staff should be aware that Internet traffic is monitored (and automatically reported by School Care) and can be traced to the individual user. Discretion and professional conduct is essential.*
* *Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.*
* *All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.*
* *All members of the school will use complex passwords for logging into the school server (except class accounts which have no password)*
* *Staff with laptops shall have complex passwords which are not written down or shared with anyone else.*
* *Staff allocated a school iPad or other mobile device must secure it with a complex password*
* *Staff must not use personally owned mobile phones (or other devices) to access school personal data*
* *Breaches of the Policy should be reported to the designated Safeguarding Lead (Or other Designated Safeguarding Officer) in the first instance.*
	1. **Policy in Practice- Parents**

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

Schools may wish to refer parents to websites referred to in the references section of this document.

* *Parents’ attention will be drawn to the Online Safety Policy and RUP in newsletters, school prospectus and Website.*
* *A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.*
* *Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.*
* *Internet issues will be handled sensitively to inform parents without undue alarm.*
* *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*
	1. **Handling of complaints**

Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school’s behaviour policy. All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc. Complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures.

* *Responsibility for handling incidents will be delegated to a senior member of staff.*
* *Any complaint about staff misuse must be referred to the head teacher.*
* *Pupils and parents will be informed of the complaints procedure.*
* *Parents and pupils will need to work in partnership with staff to resolve issues.*
* *There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.*