Widford Lodge

PREPARATORY SCHOOL

eSafety and IT Security Policy

This policy applies to all pupils in the school including those in the EYFS

Date reviewed and approved by the Proprietor: September 2018
Next Review: September 2019

Introduction

ICT in the 21st century is an essential element for education, business and social interaction and forms part of the everyday lives of pupils, their parents and staff. Widford Lodge recognises the risks associated with such technology but believes that the benefits outweigh these and so we are committed to:

- Establishing ground rules for using technology whilst at school
- Educating pupils, parents and staff on esafety
- Teaching pupils how to behave and think to enable them to remain safe and legal, both inside and beyond the classroom
- Filtering the websites, networking and downloading available to all those who use the internet whilst on the school site.

We hold and process personal data about pupils, staff and parents/guardians for the purposes of:

- Administration
- Academic progress monitoring
- Organisation of school functions
- Historic records
- Student welfare
- Health
- Statistics and research.

We recognise that some of this information is sensitive and we intend to fully comply with the General Data Protection Regulations 2018. Everybody at Widford Lodge School has a shared responsibility to secure and process correctly any sensitive information.

The purposes of this policy therefore are to:

1. Clearly define roles and responsibilities for online safety and how this links with our wider safeguarding strategy
2. Give clear guidance on the use of technology in the classroom and beyond, for all users, including staff, pupils, parents and visitors and outline restrictions and sanctions
3. Detail the school's technical provision and safeguarding mechanisms for filtering, monitoring and reporting inappropriate content
4. Detail how we build resilience in pupils to protect themselves and their peers through education and information
5. Outline the training and guidance given to staff with regard to online safety
6. Detail the reporting mechanisms for users to escalate issues and concerns and how these are managed
7. Outline how we inform, communicate with and educate parents/carers in online safety
8. Outline how personal data is managed in line with statutory requirements.

This policy is available on the school's website and should be read in conjunction with other policies, including our Safeguarding and Child Protection policy, our Data Protection policy, our anti-bullying policy and our policy for the promotion of good behaviour.

1. Roles and Responsibilities for Online Safety

The Headteacher and Proprietor have ultimate responsibility for ensuring that this policy and the practices detailed within it are fully implemented and followed. The Designated Safeguarding Lead is Sam Pawsey and it is part of her role, along with Andrew Blundell (Digital Learning subject leader) to keep abreast of current issues and to take prompt and appropriate action as necessary. Online safety and safeguarding children in their use of technology are vital parts of our wider safeguarding strategy, as detailed throughout this policy.
The Digital Learning subject leader routinely monitors the school's online reputation. Should anything be found that brings the school into disrepute, it will be reported to the Headteacher immediately and appropriate action taken.

2. Guidance on the use of Technology for all users

All staff are aware of the risks associated with technology and of the potential for misuse. The expectations placed on pupils are explained regularly and appropriately as their use of and exposure to technology widens.

Children are only allowed to use the internet on the school site while a responsible adult is present.

All parents of pupils joining the school are asked to read and sign the internet agreement (see Appendix A). Once pupils reach Form 3, and again in Form 5, they are also asked to read and sign the pupil internet agreement and are responsible for their own behaviour, including the materials they choose to access and the language they use. By signing this agreement, they are made aware of the restrictions on their online activity. Using technology sensibly and adhering to the internet agreement is a school rule and therefore forms part of our Policy for the Promotion of Good Behaviour. As such, any breaches are dealt with appropriately and sanctions applied according to the nature and severity of the incident.

Pupils have the opportunity to use edmodo – an online learning space designed specifically for schools. edmodo allows pupils and teachers to communicate with each other through posting messages, uploading pictures, attaching files or links. Pupils can only access and send messages to groups that have been set up and moderated by teachers. There is no private messaging between pupils. Teachers can edit or delete messages if necessary. Pupils must use standard English and follow politeness conventions. Such messaging is monitored by the relevant teacher for each group.

As part of the Computing curriculum, in every year group pupils receive advice on the benefits and risks of technology (see section 4 below).

Staff members are made aware of the school's procedures for safeguarding upon appointment. They are given guidance on how to use technology effectively and of the risks associated as part of ongoing training (see section 5 below). All staff are also made aware of the school's policy for the use of cameras, mobile phones and other wireless technology. All staff sign an acceptable use policy outlining their responsibilities and restrictions for the use of technology on the school site and for school related matters offsite and are therefore aware that they can be disciplined for any breaches of this policy.

When visitors sign into the Office, they are made aware of our online safety procedures, including the fact that they may not photograph or video children without prior permission, or access inappropriate material while on school premises.

<u>Information and Communication Systems</u>

The school's electronic communications and equipment are intended to promote effective communication and working practices. Staff are required to comply with this policy and the acceptable use of technology agreement they sign on appointment and any breaches of these documents are regarded as disciplinary offences.

The school is required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights as well as the General Data Protection Regulation.

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password of appropriate strength, which they must keep confidential. Staff are required to log off from desktops or laptops when leaving the room to prevent unauthorised users accessing the system in their absence. Staff who have been issued with school laptops or iPads must ensure that they are kept secure at all times and that passwords are used to secure access to data, as well as ensuring they do not use or display such equipment in dangerous or public areas.

Staff may not download, install or run software from external sources without obtaining prior authorisation. Chat rooms, social networking sites and webmail should not be accessed from the school network because of their potential to overload the system or introduce viruses. Mobile devices or equipment should not be attached to the school's systems without prior approval.

Staff should be cautious when opening emails from unknown external sources or where an email appears suspicious. The Headteacher should be informed immediately if a suspected virus is received. The school reserves the right to block access to attachments to email. Staff should always consider if email is the appropriate medium for a particular communication; emails should be written as professionally as a letter, with appropriate content and language used. Emails should never be sent in the heat of the moment or without considering how the message is likely to be received and staff should review carefully, seeking the views of senior colleagues as appropriate.

Staff should remember that emails can be the subject of legal action in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff and the school. All email messages should be treated as potentially retrievable, even when they have been deleted. Any member of staff who receives a message that is offensive, abusive, discriminatory or defamatory should report it to the Headteacher. The school recognises that it is not always possible to control incoming mail.

As detailed in this policy, the school uses a filter for the internet, which prevents access to inappropriate sites wherever possible. Staff should not attempt to access while at school or at home using school hardware any web page or files which could be regarded as illegal, offensive, in bad taste or immoral.

The school permits the incidental use of its internet, email and telephone systems for personal use however this is a privilege and not a right and can be withdrawn or amended at any time. Use should be minimal, not interfere with school commitments and fall within the guidelines outlined in this policy. Misuse or abuse of this permission will result in disciplinary action being taken.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. Viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities, will amount to gross misconduct:

- Accessing pornographic, racist, inappropriate or unlawful materials
- Transmitting a false/defamatory statement about any person or organisation
- Sending, receiving, downloading, displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence or embarrassment or harass others
- Transmitting confidential information about the school and any of its staff, pupils or associated third parties
- Transmitting any other statement likely to create any liability for the employee or the school
- Downloading or disseminating material in breach of copyright
- Engaging in on line chat rooms or online gambling
- Forwarding electronic chain letters and other materials
- Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

3. Technical Provision and Filtering/Monitoring

Technical Overview

Widford Lodge's IT infrastructure is built on Microsoft Active Directory domain. This provides security and auditing for each user/pupil. Access to data resources are provided by security groups, whilst Group Policies maintain application and desktop control.

Web Monitoring and security is provided by a Barracuda appliance sitting in series with the Cisco ASA 5505 Internet Firewall. This controls and audits any Internet requests from any device that connects to the school's

network (Tablet, PC, server etc.) This gateway device ensures there is no way to avoid what the school's internet policies enforce. Automated alerts are sent to the network administrator for investigation.

All PCs are Windows 10 Educational or Professional and must be part of the security domain to gain access to network resources (providing user logging on has relevant security rights assigned to them).

PCs have Sophos Data Protection suite which provides AV, malware & 2nd line web defence to block unwanted websites. Sophos is controlled and monitored by a central server residing on the Domain controller. Any security or AV alerts are sent direct to the Network Administrators for investigation.

iPads are managed via a Mac-Mini server running Apple Configurator. This restricts user access to system settings and ensure only authorised applications are installed onto devices via use of assigned policies.

One physical HP Hyper-V server which hosts 4 virtual Microsoft Windows 2016 Servers.

Email is provided by Microsoft Office 365 (cloud based exchange server) and secured by SSL certificates for Outlook Web Access (phones & web mail if enabled for user). Multiple email spam & malware protection is provided within Office 365.

Office 365 also provides a cloud based file sharing environment (SharePoint online) which allows access to essential files (i.e. if School Internet service goes down, or physical access problems prevent connection to the school's server). Office 365 provides full auditing & lock down of file access for data compliance.

Data Backups

All data is automatically backed up overnight to an online secure encrypted location. Encryption is FIPS 140-2n compliant.
SQL server is backed up daily to an online secure encrypted location.
Office 365 (email & SharePoint) is backed up within the cloud automatically.

Internet Security

Internet security is provided by an enterprise class Cisco ASA 5505 Firewall.
Web security & filtering is provided by a Barracuda 410 appliance which receives hourly content filtering updates. A weekly report of any attempts to access blocked sites, such as adult content, violence/terrorism/gaming is reviewed by the Senior Management Team and dealt with appropriately. At any time, the Headteacher or Designated Safeguarding lead can request Soft Egg to produce reports of the online activity of any user or group of users.

Any issues raised by filtering or monitoring are dealt with promptly and sensitively.

Sophos Web filtering provides 2nd line of defence.

Staff are aware of the need to report immediately any instances of inappropriate content to the Digital Learning Leader, who will inform the Headteacher and Soft Egg.

Server & firewall Security Update schedule

All Microsoft server operating systems are updated weekly.
All clients are update weekly and controlled by WSUS server
Sophos – Updated hourly and pushed to the clients every 2 hours
Barracuda – Updates received every hour
Cisco ASA – Updates applied where Cisco advisories are posted
Office 365 – Updated automatically by Microsoft
SharePoint Online - Updated automatically by Microsoft

Software

All software within the school is legally licensed and copies of the licences are held centrally. No software is ever installed which might compromise the security of the IT system. All software is acquired from legitimate publishers/re-sellers.

4. Building Resilience in Pupils

As detailed in section 2 above, all pupils are required to sign an internet agreement at the start of Form 3 and Form 5. As part of the Computing curriculum, pupils receive regular and age-appropriate guidance on safe and legal internet use and what to do they are unhappy with anything they come across. A specific esafety afternoon is held for Year 6 children in the term before they move onto senior school. Brief details are listed below, further information is available in the curriculum booklets on the school website or from the Digital Learning Leader.

Form 1 Hector's World – What is personal information and when should it be given out; how to identify people who can be trusted; understanding situations which may become risky online and what to do

Form 2 Lee and Kim's Magical Adventure – Keeping Safe on the Internet

Form 3 Learning: the purpose and safe use of technologies, keeping personal information secret; how to deal with inappropriate material (Zip-It, Flag-It, Block It!); and how to be S.M.A.R.T. in the online world.

Form 4 CEOP Cyber Café & Band Runner Game – interactive e-safety resources highlighting how to stay safe from online risks How to: protect your online reputation, avoid seeing things online that could upset you, avoid getting viruses, and to think before you post; promote positive behaviours in the online world; what do your online pictures say about you?

Form 5 Learning how to stay safe from sexual abuse, exploitation and other risks they might encounter online; using social networking safely; understanding that profiles should be set to private; to only talk to people who are known and trusted in the real world and what to do if things go wrong (Play-Like-Share & Jigsaw); and taking control of your digital footprint

Form 6 Learning about the dangers of social media, sexting and sharing (very) personal images, keeping important information private; and recognising what positive and negative online behaviour is, how it can impact others' feelings and how to develop strategies to resolve online disagreements in a positive and healthy way. Think-U-Know Who You're Talking To? – CEOP presentation

5. Training and Guidance for Staff

Staff members receive guidance as part of their induction and at least annually as part of their ongoing professional development. Contracts of employment require teachers to agree to the school's procedures for the use of technology.

6. Reporting Mechanisms

A member of the Senior Management Team may inspect, or ask SofteggT to inspect, any ICT equipment owned or leased by Widford Lodge at any time without prior notice. They may also monitor, intercept, access, inspect, record and disclose telephone calls, emails, messages, internet and any other electronic communications involving Widford Lodge employees or contractors, without consent, to the extent permitted by law. Any such activities will comply with the General Data Protection Regulation 2018, the Human Rights Act 1998, the Regulation of Investigation Powers Act 2000 and the Lawful Business Practice Regulations 2000.

Any breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school hardware, software or services. Any policy breach is grounds for disciplinary action and may also lead to criminal or civil proceedings.

Staff, parents and pupils must report any security breaches or attempts, loss of equipment or unauthorised use or misuse of ICT to the Headteacher or Designated Safeguarding Lead.

All esafety incidents will be logged on the safeguarding concerns file.

Accidental access to inappropriate materials by pupils or staff should be reported to the Digital Learning leader, who will inform the Headteacher and Softegg.

Any concerns, complaints or issues raised with regard to esafety will be recorded and actioned promptly and in line with the relevant policies.

7. Communication and Education for Parents

Parents are invited to attend annual esafety sessions run by the Digital Learning leader, as well as having to sign an internet agreement when their child joins the school. They are welcome to raise any concerns with the class teacher, the Digital Learning leader or the Designated Safeguarding Lead, which will be dealt with promptly and appropriately.

8. Management of Personal Data

As detailed in the introduction to this policy, Widford Lodge holds and processes personal data about pupils, staff and parents/guardians for a variety of reasons and takes seriously its responsibility for this data.

Parents sign to give permission for images of their children to be used and stored for a variety of purposes: where such permission is not given, all relevant members of staff are made aware.

Electronic data is protected by password and firewall systems. Computer workstations in administrative areas are positioned so that they are not visible to casual observers. Similarly, data stored in paper form is stored securely and where it is not easily accessible to anyone without a legitimate reason to see it.

Personal data will only be disclosed to organisations or individuals whose identity has been verified and for whom consent has been given to receive the data, or to organisations that have a legal right to receive it without consent being given.

Full details of our data protection procedures are detailed in our Data Protection Policy.

Appendices

A – Pupil and Parent Internet Agreement

B – Legislation relevant to esafety

C – Useful references/Information

Widford Lodge

PREPARATORY SCHOOL

Use of the internet: Home–School Agreement (Parents' Copy)

- All pupils are expected to read and agree the Internet Agreement and to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher
- Pupils are expected not to use any inappropriate language in their e-mail communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending or the passing on of chain letters
- Pupils must ask permission before accessing the Internet
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc or CD Rom should be brought in from home for use in school.
- Homework completed at home may be brought in on a memory stick but this will have to be virus scanned by the class teacher before use.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters)
- No personal information such as phone numbers and addresses or any part thereof should be given out and no arrangements to meet someone made unless this is part of an approved school project
- Pupils choosing not to comply with these will be denied access to Internet resources.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Widford Lodge

PREPARATORY SCHOOL

Responsible Internet Use (Pupil Copy)

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my own network login and password.
- I will only look at or delete my own files.
- I understand that I must not bring software or disks into school without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Widford Lodge

PREPARATORY SCHOOL

Responsible Internet Use
Consent Form

Please complete, sign and return to the school secretary

Pupil's Agreement

Pupil: *Form:*

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: *Date:*

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand 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.

Signed: *Date:*

Please print name:

Dear Parents

Responsible Use of the Internet

As part of your child's curriculum and the development of ICT skills, Widford Lodge Preparatory School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please contact the School Office to arrange an appointment.

I would ask you to look through these rules and discuss them with your child and then return the signed form to us at school.

Thank you for your co-operation

Yours faithfully,

Appendix B – Legislation Relevant to Esafety

The Independent School Standards Regulations 2014

General Data Protection Regulation 2018

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Regulation of Investigatory Powers 2000

Human Rights Act 1998

Racial and Religious Hatred Act 2006

Sexual Offences Act 2003

Communications Act 2003 (section 127)

The Computer Misuse Act 1990

Malicious Communications Act 1988

Copyright, Design and Patents Act 1988

Public Order Act 1986

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964

Protection from Harassment Act 1997

Freedom of Information Act 2000

Appendix C - Useful references/Information

National Action for Children (NCH) **www.nchafc.org.uk/itok/**
Parents Guide on Internet usage

Bullying Online **www.bullying.co.uk**
Advice for children, parents and schools

FKBKO - For Kids By Kids Online **www.fkbko.co.uk**
Excellent Internet information for KS1 to KS3

Parents Information Network (PIN) **www.pin.org.uk**
Comprehensive guidelines on Internet safety

Parents Online **www.parentsonline.gov.uk/2003/parents/safety/index.html**
Interactive learning and safety advice, excellent presentation for parents.

Kidsmart **www.kidsmart.org.uk**
An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? **www.thinkuknow.co.uk/**
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Family Guide Book (DfES recommended) **www.familyguidebook.com**
Information for parents, teachers and pupils

NCH Action for Children **www.nchafc.org.uk**
Expert advice for children, young people and parents.

Safekids **www.safekids.com**
Family guide to making Internet safe, fun and productive

Associations of Co-ordinators of IT (ACITT) **www.g2fl.greenwich.gov.uk/acitt/resources/assoc/aup97.doc**
Acceptable use policy for the Internet in UK Schools, original straightforward text.

NAACE / BCS **www.naace.org** (publications section)
A guide for schools prepared by the BCS Schools Committee and the National Association of Advisers for Computer Education (NAACE)

DfES Superhighway Safety **http://safety.ngfl.gov.uk**
Essential reading, both Web site and free information pack. Telephone: 0845 6022260

KS2 Internet Proficiency Scheme **www.becta.org.uk/corporate/corporate.cfm?section=8&id=2758**
A Becta, DFES and QCA pack to help teachers educate children on staying safe on the internet

Internet Watch Foundation - **www.iwf.org.uk**
Invites users to report illegal Web sites

Data Protection **www.informationcommissioner.gov.uk/**
New Web site from the Information Commissioner

Kent Web Skills Project **www.kented.org.uk/ngfl/webskills/**
Discussion of the research process and how the Web is best used in projects.

Click Thinking: Scottish Education Department **www.scotland.gov.uk/clickthinking**
Comprehensive safety advice

Kent ICT Security Policy **www.kent.gov.uk/eis** (broadband link)
An overview of the need to secure networks with Internet access.

Copyright **www.templetons.com/brad/copymyths.html**
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.

Internet Users Guide **www.terena.nl/library/gnrt/**
A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web.

Alan November – The Grammar of the Internet **www.edrenplanners.com/infolit/**
Article explaining how to evaluate Web sites and information

DotSafe – European Internet Safety Project **http://dotsafe.eun.org/**
A comprehensive site with a wide range of ideas and resources, some based on Kent work.

Cybercafe **http://www.gridclub.com/home_page/hot_headlines/cyber.shtml**
Internet proficiency through online games for KS2, with a free teacher's pack.