Acceptable use of ICT and Mobile Phone Policy

For School Staff and Volunteers

Approved: March 2026

Approved by: Local Advisory Board

Next Review: March 2027

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

1. Introduction

ICT is an essential part of learning and teaching, as well as everyday life, in the 21st Century. ICT covers a wide range of resources including web-based and mobile learning. At Rose Hill Primary School we encourage staff and learners to use ICT effectively and develop the use of ICT as essential life skills.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school and technologies owned by pupils and staff, but brought onto school premises.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. At Rose Hill Primary School we use it to raise educational standards, to promote pupil achievement, to support the professional work of staff, to enhance the school's management information and business administration systems and to communicate with parents.

We believe that staff and pupils will benefit from the breadth and depth of information accessible to them. Benefits include:

- Access to worldwide resources and research materials
- Educational and cultural exchanges between pupils worldwide (Skype for instance)
- Access to experts in many fields for both staff and pupils
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curricular and administration data (i.e. between colleagues, LA and DFE)

Due to the nature of the Internet and the range of information available through it, it is essential that a policy is in place to ensure the safety and well-being of all our staff and learners. We understand the responsibility to educate our pupils on on-line safety issues; teaching them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of this policy.

2. Aims of this Policy

- Allow all users access to school ICT resources and use of the Internet for educational and administrational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with UK GDPR (2018), Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with etiquette.

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

3. The Technologies

ICT has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school or used outside of school by children include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Tablets
- Other mobile devices with web functionality
- Generative AI and LLM tools are governed by the Trust's **AI Policy**; staff must follow the model-specific rules there.

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

4. Roles and Responsibilities

ICT Acceptable use/On-line Safety is recognised as an essential aspect of strategic leadership in this school and the Principal, with the support of Governors, aims to embed safe practices into the culture of the school.

- The Principal ensures that the policy is implemented and compliance with the Policy monitored. All staff will be given a copy of the policy and will sign to acknowledge that they have read and understood it.

- Governors need to have an overview understanding of acceptable use and on-line safety issues and strategies at this school. Governors will be given a copy of the policy and will sign to acknowledge acceptance of its content. The school will actively take all reasonable precautions to prevent pupils being exposed to undesirable materials. The school has invested in hardware and software infrastructures to reduce risks associated with the Internet. All Internet access is filtered through a proxy server to screen out undesirable sites at source. However, if staff or pupils discover unsuitable sites or undesirable material, they will know that they should switch off the monitor, not

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

the computer, and report the incident to the nearest teacher or the Principal who will report the URL (address), time, date and content to the Internet Service Provider. Any material that the school believes is illegal must be referred to the Trust and their advice will be acted upon. The security of the school ICT systems will be reviewed regularly. Virus protection is installed and will be updated regularly. The network manager will review system capacity regularly. The school is also committed to protecting its staff, learners, and itself from illegal or damaging actions by individuals, either knowingly or unknowingly. This requires a team effort involving the participation and support of all staff who deal with information and/or information systems. It is the responsibility of every staff user to read and understand these guidelines, and to conduct their activities accordingly.

- All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school on-line procedures. (See Appendices 1 and 5)

5. Using the Internet in class or at home

- Internet enhances learning
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for

Internet use. They are taught about cyberbullying and how to combat it

- Internet access will be planned to enrich and extend learning activities
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Evaluating Internet content
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the Principal
- Staff ensure that the use of Internet derived materials complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.
- E-mail Whole-class or group e-mail addresses should be used at Key Stage 2 and below. Pupils must not reveal personal details of themselves or others in e-mail communication.
- Social networking and personal publishing
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, academy, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the pupil or his/her location eg. house number, street name, academy, shopping centre.

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

- Pupils are advised of the laws regarding social networking sites and are told they should not be on social media sites such as Facebook if they are under age.
- Videoconferencing /Skype Videoconferencing/skyping with another school is a challenging activity with a wide range of learning benefits. It is supervised by the teacher. When video conferencing or skyping with another school, parental permission is obtained.

6. Conditions of Use

Users are responsible for their behaviour and communications. Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Staff will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Staff will report any misuse of the network to the Principal. Users are expected to utilise the network systems in a responsible manner. Appendices 2 and 3 provide some guidelines on the matter. All users are required to follow the conditions laid down in the policy. These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any use of the network that would bring the name of the school into disrepute is not allowed.

7. Unacceptable Use

Any breach of the conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users' use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter. For examples of unacceptable use see Appendix 4. Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses.

8. Personal data

We process personal and special-category data in line with UK GDPR/DPA 2018 and the DfE's data-protection guidance for schools (retention, sharing, breach reporting, SARs). Staff must only use approved systems (e.g., school email/OneDrive) for personal data.

9. Risk Assessment

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.
The school cannot accept liability for the material accessed, or any consequences of Internet access.
Methods to identify, assess and minimise risks will be reviewed regularly.

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

10. Physical Security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital, still and video cameras are secure when they are not being used.

11. School Website

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner. The contact details for the school will include only the school's postal address, e-mail address and telephone number. No personal information of staff or pupils will be published.

The school will not publish photographs of pupils without a parent or carer's permission, in line with the school's photography policy. A pupil's name will not be used in association with photographs.

12. Mobile Phones

The aim of this section is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines. We understand that pupils may bring mobile phones to school. The pupils hand these in to the school office where they are kept until the end of the day. As a general rule staff will not make or receive calls or texts during lesson time or meetings. Phones will be kept on silent during these times. This is to avoid distraction and disruption during lessons and meetings. Phones will not be used in a space where children are present e.g. classroom, playground. This will avoid adults putting themselves into compromising situations which could be misinterpreted and lead to possible allegations. There may be exceptional circumstances when staff need to keep their phones on as a necessary reassurance. Such use will be for an agreed limited period until issues or concerns leading to the exceptional circumstance request have been resolved such as medical tracking on mobile devices or as the DSL for professional contact. It is ensured that at all times the school landline is available for emergency or urgent contact.

We implement a phone-free environment by default during lessons, transitions, and breaks, with reasonable adjustments for SEND/medical needs. Staff model expectations (no personal phone use in front of pupils)

13. Social Networking

This section aims to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines. Social Networking through internet sites such as Face Book has become more and more popular over the last few years. The vast majority of staff and parent have social network accounts which are used responsibly.

To avoid adults putting themselves into compromising situations, which could lead to allegations and to protect the whole community from being identified on social networking sites, the following list of list of Do's and Don'ts of acceptable use have been established:

DO

- Select your "friends" carefully and consider who is able to see your profile – remember that friends of your friends may sit with them at a computer or may be given access without you knowing.
- Limit access to your profile to only your "friends"; ensure that your privacy settings are always up to date – the social networking providers change the setup of these frequently.
- Ensure that the privacy settings on your photo albums are set to "friends only".

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

- Ensure comments/photos/videos of yourself that may be posted by you or others do not show you in a way that could be construed as unprofessional for a member of staff/volunteer working in a school.
- Consider carefully the "groups" that you may join and are then shown on your profile.

DO NOT

- Accept children (under the age of 18) that you have met/taught in the course of your profession as "friends".
- Upload photos/videos of school activities that involve children or jeopardise the professional status of others.
- Post any comments of any nature about children and/or parents in the school.

14. How will complaints regarding On-Safety be handled?

The school will take all reasonable precautions to ensure On-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Any complaint about staff misuse is referred to the Principal. Complaints of cyberbullying will be dealt with in accordance with the school's anti-bullying policy. Complaints related to child protection will be dealt with in accordance with the school's and Local Authority child protection procedures.

Use of school systems may be monitored/logged for security and safeguarding. Where concerns are raised, an investigation will follow a defined process (initial triage → evidence preservation → outcome), with outcomes ranging from coaching to disciplinary action. Records are managed in line with data-protection guidance.

15. Parental Support

Parents' attention is drawn to the school Acceptable Use/On-Line Safety Policy in induction packs and on the school website.

16. Personal Data Breaches & Subject Access Requests (SARs)

Personal Data Breaches — staff duties and process

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (including special-category data). All staff must:

1) Report immediately: If you suspect or become aware of a breach (e.g. mis-sent email, lost device, phishing click, unauthorised access), inform the DPO/Principal at once and log the incident via the school's breach route. Do not attempt to fix or "quietly" resolve the issue yourself.

2) Preserve evidence: Do not delete emails/files, wipe devices, or alter logs. Capture key facts (who/what/when/how) and keep any related materials secure for investigation.

3) Follow the investigation: Cooperate with the DPO/IT investigation, including containment, risk assessment, and lessons-learned actions (e.g., password resets, user notifications).

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

4) Regulatory timescales: The school will assess whether the breach must be reported to the ICO within 72 hours and whether affected individuals must be informed; staff must provide requested information promptly to meet statutory deadlines.

5) Tools & systems only: Always process personal data using approved school systems (e.g., school email/approved cloud storage) and in line with our retention, sharing and security procedures.

Subject Access Requests (SARs) & other information rights

Individuals (or those with parental responsibility, where applicable) have the right to access their personal data. To ensure lawful, timely responses:

1) Pass SARs on immediately: Any request for personal data (written, email or verbal) must be forwarded the same day to the DPO/Principal; do not disclose information yourself.

2) One-month response: The school normally has one month to respond to a valid SAR (extendable in limited cases). Staff must help the DPO locate records quickly (emails, files, MIS entries, chat logs, CCTV where applicable).

3) Secure handling: Provide only through approved channels; apply redaction where required; never download school personal data to unapproved devices or personal accounts.

4) Other rights: Requests to rectify, erase, restrict or object must also be sent to the DPO immediately; do not action independently.

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

Oxlip LEARNING PARTNERSHIP

Appendix 1: With Children

Staff need to:

- Make pupils aware of appropriate behaviours when using the Internet
- Remind children of the rules for using the Internet, including social media use
- Watch for accidental access to inappropriate materials and report the offending site to the Principal. If undesirable material is discovered, switch off the monitor, not the computer.
- Check before publishing children's work on the school web site to make sure that the school has parental permission
- Report any breaches of this policy to the Principal
- Ensure safe use of e-mail
- Ensure safe use of school network, equipment and data
- Ensure safe use of digital images and digital technologies, such as mobile phones, phone and digital cameras
- Be aware that e Bullying / Cyberbullying can take place out of school
- Be aware of their role in providing On-line-Safety education for pupils
- Be aware that e-mail addresses are created for a whole class or teaching groups, not for individuals

Appendix 2: Personal use by Staff

- Internet access in all schools is filtered to prevent the viewing and downloading of inappropriate material. Do not attempt to access inappropriate sites. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Please respect other people's material and do not corrupt, interfere with or destroy them. Do not open other people's files without express permission.
- If your username and password are unique to you so do not give them to anyone else. Always remember to log out and close the browser when finished. If you think someone has learned your password then contact the Principal.
- Do not release or in any way make available personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) over the Internet. School email addresses should be used for school based communications.
- When working with SIMS or any other personal data ensure that the data is secure.
- Do not take digital photographs or videos using your personal digital cameras or mobile phone cameras
- Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

Appendix 3: Network Etiquette and Privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages that are likely to cause annoyance, inconvenience or needless anxiety.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Make sure nothing in the messages could be interpreted as libellous.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.
- Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
- Do not attempt to visit websites that might be considered inappropriate.
- It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

Appendix 4: Examples of Unacceptable Use

- Accessing or creating, transmitting, displaying or publishing any material e.g. images, sounds or data that is likely to cause offence, inconvenience or needless anxiety.
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data. Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
- Any use of the network that would bring the name of the school into disrepute is not allowed.

Appendix 5: Pupil On-Line Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when emailing.
- I will only open e-mail attachments from people I know, or whom my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my On-Line Safety.
- I will not join any social media sites if I am under the age limit.

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

Oxlip LEARNING PARTNERSHIP

Appendix 6: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

Appendix 7: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**

Appendix 8: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

T: Ipswich Campus 01473 277243 / Mid-Suffolk Campus 01449 742422 E: mail@oxlip.uk **www.oxlip.uk**