Online Safety Policy

(Including internet access and Acceptable use of technology agreement)

Approved by Governing Body on: 6/9/21

Signed chair of governors:

Head Teacher: Amy Findlay

Next Review: September 2022

Vision Statement

Opportunities for all

Realising the child's potential

Challenging and exciting

Holistic, happy and healthy

Aspirational

Recognising and celebrating achievements

Diversity and partnership

Mission Statement

Together with home and the community, we aim to provide a nurturing, challenging, high quality teaching and learning environment within a friendly, supportive multi-cultural setting. Encouraging children and staff to respect and value one another.

Contents

1. Introduction

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe internet access.

This policy considers the four areas of risk within online safety, which are:

- Protecting users from illegal/inappropriate/harmful content
- Protecting users from harmful online interaction/contact
- Policies for personal online behaviour/conduct
- Minimising risk from commerce

2. Rationale

- The school aims to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our children and will, in return, expect staff to agree to be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- ICT access will also be provided when appropriate for governors, volunteers and visitors, and they will also be expected to read and sign an acceptable use agreement.
- It is expected that our children will only use school ICT whilst being supervised. If mobile technology is provided for use at home the parents will be asked to sign the home- school agreement
- Online safety measures regarding mobile technology used both on-site and off-site are described in this document.
- Information security measures relating to School ICT will be taken by the school
- The aim is to protect the School ICT systems and users from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Incidents of misuse will be investigated. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. They could if necessary, include disciplinary or safeguarding processes. A referral to the police will be made if criminal activity is detected.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, Sept 2021 and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and health education
- Searching, screening and confiscation
- It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum ICT teaching agenda.

4. The Technologies

ICT in the 21st Century 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 and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking site
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

5. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive Online Safety education programme for staff and parents through face to face and online information and for pupils via the relationships and health education curriculum provision.

6. Staff Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head Teacher, with the support of DSL and the Governing Body, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to raise concerns as they arise with the ICT team, DSL or HT as appropriate. All visitors also receive Online Safety information on arrival at school.

The responsibility for Online Safety has been designated to a member of the senior leadership team; Barbara Ackerley as DSL with the support of Mark Ridgway as ICT Network and Services Manager.

Our Online Safety Coordinators ensure they keep up to date with Online Safety issues and guidance through liaison with other organisations/professionals. The school's Online Safety Coordinators ensure the Head, Senior Management and Governors are updated as necessary.

6.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Body will nominate a governor to oversee online safety. The nominated Governor is Helen Grindulis Responsibilities will include arranging regular meetings with appropriate staff to discuss online safety, and monitor any incidents of misuse of ICT.

All governors will ensure that they have read and understand this policy, and will agree and adhere to the terms on acceptable use of the school's ICT systems and the internet. See Acceptable Use of Technology section 8 and Appendix 1 below

6.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

6.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in the safeguarding policy.
The DSL takes lead responsibility for online safety in school in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT Network and Services Manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately (See sections 11 to 13 below and also the Acceptable Use of Technology Policy).
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and if necessary the Governing Body.

6.4 The ICT Network and Services Manager

The ICT Network and Services Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Helping to ensure that any online safety incidents are logged (See section 11 below and also the Acceptable Use of Technology Policy) and dealt with appropriately in line with this policy.
- Producing weekly Internet Monitoring Reports, that contain attempted access to sites in blocked categories related to safeguarding and any searches made that hit keywords from a list related to safeguarding
- Investigating anything that appears on this reports and reporting anything that is still a concern to the Designated Safeguarding Lead.

6.5 All Staff and Visitors

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the school's terms on acceptable use of the school's ICT systems and the internet, (See section 5 below and also the Acceptable Use of Technology Policy).
- Teaching and support staff will need to support pupils when they are using ICT.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- The visitors leaflet clearly outlines Online Safety and acceptable use of technology information relevant to supply staff, volunteers and contactors.

6.6 Parents

Parents are expected to:

- Be aware of the measures The School takes to ensure ICT safety.
- Follow Acceptable Use guidance if their child has home use of any mobile technology provided by The School and sign an agreement regarding this. (Appendix 2 below)
- School will provide parents with information on online safety as part of the Relationships and Health Education curriculum, to support parents in keeping their children safe online. There is a section on the school website dedicated to this.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

If concerns or queries about this policy are raised with another member of staff they should report this to the headteacher or DSL.

6.7 Visitors including volunteers

Visitors, such as training providers, who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. This will sent out with the room booking.

Relevant information is within the volunteer handbook.

7. Training

7.1 Staff

- All staff receive regular information and training on Online Safety issues in the form of in house training which includes online and face to face training.
- New staff receive information on the school's Acceptable Use agreement as part of their induction. See section 8 and Appendix 1 below.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas as is appropriate and through a culture of talking about issues as they arise.
- Online Safety records of concern are completed by staff as soon as incidents occur and are reported directly to the school's designated safeguarding team.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures.

7.2 Parents

- School will provide parents with information on online safety as part of the Relationships and Health Education curriculum, to support parents in keeping their children safe online. There is a section on the school website dedicated to this.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

7.3 Children

- Children are taught how to use ICT responsibly within the curriculum (appropriate for their developmental level.) They are specifically taught about inappropriate use within the Relationships and Health Education curriculum.

8. Acceptable use of ICT in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Parents will be expected to sign an agreement if their child is given any school mobile technology to use at home. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Our children only use ICT under supervision, and do not bring personal mobile technology into school. The filtering systems give protection against being exposed to illegal/inappropriate/harmful content, sites linked to harmful interactions, and sites that have a risk when it comes to commerce. The staff supervision also helps in these areas as well as reducing any risks caused by conduct (such as preventing making/sharing/receiving of explicit images).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
Staff will be allocated password protected access to the school ICT system. They should ensure their password meets the complexity requirements. They should not tell anyone their password, write it down on paper or on e-mail, or share it with others. They should not log on using anybody else's account and they must ensure that they log off or lock the screen when leaving a computer. Others should not share use of the system using a single password.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Additional software must not be downloaded onto school devices without consent (discuss with the ICT Network and Services Manager if there is a piece of software you require related to your work).

8.1 Mobile Technology use in school

This relates to use of laptops, tablets and handheld computers

Staff should ensure that mobile technology is locked when left unattended to prevent unauthorised access. It should be locked away securely at the end of the session.

Staff personal devices (e.g. phones, tablets, laptops, PDAs) should only be used in areas where no pupils will be present. They should be kept on silent and locked away at other times.

Any device that is accessed by a pupil must go through the school's broadband connection that provides appropriate content filtering and monitoring. None of the devices provide any support for cellular connectivity and hence must do through the school's Wi-Fi or be connected to the school network by ethernet. Pupils are not allowed to use their own mobile devices in school.

8.2 Mobile Technology use out of school

Staff members using a work device outside of school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Work devices are provided solely for work activities.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school and must not let anyone else use the school laptop for any purpose.

Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek immediate advice from the ICT Network and Services Manager.

9. Network security

9.1 Internet

The Orchard School uses a Sophos XG Firewall, which will minimise the chances of pupils encountering undesirable material. This includes content filtering that blocks various categories of websites to users, thereby blocking access to illegal, inappropriate, and harmful content, sites linked to harmful online interaction, as well as sites associated with commerce (such as gambling, inappropriate advertising, phishing, and scams). The firewall also includes a reporting section, so that we can monitor for any inappropriate use.

- Staff, pupils and visitors have access to the internet through the school's fixed and wireless internet technology.
- Staff should email school-related information using their @orchard.sandwell.sch.uk address and not personal accounts.
- Staff will preview any websites before recommending to pupils.
- Internet searches are conducted using the Safe Search – central policies on the firewall/server enforce this.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the online safety coordinator(s) detailing the device and username. The ICT Network and Services Manager will be informed so this can be investigated.
- Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.
- 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 and then The ICT Network and Services Manager who can block further access to the site.
- Pupils are taught about email and the need to use appropriate inoffensive language in messages if their developmental level is such that this is relevant. They are also taught not to give any personal information such as phone numbers and addresses.

9.2 Passwords

- Use a strong password (strong passwords are usually eight characters or more, contain three or more of upper case letters, lower case letters, numbers, symbols and Unicode characters, and do not contain three or more consecutive characters from the username.
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

9.3 Mobile technology security

Staff school laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.

- Staff should only use the laptop which is allocated to them.
- Mobile technology devices for pupil use, are stored in a locked cupboard. Access is available via classroom staff.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during staff break times only, in rooms where no pupils have access and kept on silent in locker or class cupboard.

10. Data storage

- Data relating to work in school should be stored in files on the school server or school cloud service. It should not be stored on the hard drive or storage area of any computer/laptop/tablet/handheld device or unapproved removable media. Any photos taken on devices should transferred to the school server/cloud service as soon as is reasonably possible.
- Removable devices should not be used as a permanent data store. Only an approved encrypted USB flash drive will be provided by the ICT Network and Services Manager to use if necessary (with a secure password) to transfer files between devices.
- DVDs are used to store evidence of pupil learning and often includes photos and video footage relating to individual pupils. These are stored within school and are not to be removed from the premises without permission.

11. Social Networking Sites

- Roles in school requires a high degree of professionalism and confidentiality
- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends/contacts, unless known to you as a friend or relative prior to your appointment to post within The Orchard School.
- Under the remit of safeguarding, we ask that you tell the DSL if you have regular contact with families which requires you to share contact information e.g. respite care
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression applies only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;

- bring the School into disrepute;
- breach confidentiality;
- breach data protection legislation
- breach copyright

Users of social networking media should not communicate anything that could be considered discriminatory against, or cause bullying or harassment of any individual, for example by:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, age, religion or belief.
- using social media to bully another individual; or
- posting images that are discriminatory or offensive or links to such content.

Any communications or content published that causes damage to the school. Local Authority, any of its employees of any third party's reputation may amount to misconduct or gross misconduct to which the school's disciplinary policy applies.

12. Cyber-bullying

Our children are unlikely to understand what cyber-bullying is, or to carry it out themselves, though they may still be exposed to it by others.. They will be taught about it as developmentally appropriate within the personal, social, health education curriculum.

Parents will also be advised about this within online safety awareness raising

13. Published Content and Use of Images

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for children's' evidence of work, notice boards, school brochures or website materials. We will clearly explain how the photograph and/or video will be used to the parent/carer.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When taking photos or videos the school equipment should be used. It is not permitted to use personal equipment. This includes integral cameras on mobile phones.

When staff select photos/videos for inclusion on the website they must check that the photos are both suitable and that the child(ren) have permission to appear on the website. When staff compose any text to go on the website, they must make sure this does not contain any names or other personal information.

Although a large number of staff can provide content for the website, only certain members of staff have permission to update it and they each have their own account to do this.

14. Monitoring

The Head Teacher/Deputy Head Teacher or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the GDPR, or to prevent or detect crime.

15. Breaches of Practice

A referral to the police will be made if criminal activity is detected. Any policy breaches will be investigated. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. This could if necessary include disciplinary or safeguarding processes. Such breaches may also lead to criminal or civil proceedings.

The School reserves the right to monitor staff internet usage and behaviour relating to use of social media. The School considers that valid reasons for this include concerns that social media/internet sites have been accessed in breach of this Policy.

16. Incident Reporting

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Lead or ICT Network and Services Manager.

17. Links with other policies / documents

This Online Safety Policy is linked to:
Data Protection policy
Safeguarding policy Sept 2021
Staff disciplinary procedures
KCSIE September 2021

APPENDIX 1

Acceptable Use of Technology Agreement for Staff, Governors, Volunteers, Visitors.

These rules are designed to protect staff and visitors from Online Safety incidents and promote a safe e-learning environment for pupils.

General Principals

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that the young people receive opportunities to gain from the use of ICT. I will, where appropriate, educate the children in my care in the safe use of ICT.
- I understand that this Acceptable Use agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment (e.g. laptops, tablets, handheld devices, email, other online services etc.) out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I do not follow this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the case of illegal activities the involvement of the police.
- I understand my responsibilities under the terms of GDPR

Use of School Devices

- I understand that the school ICT systems (both hardware and software) are for educational use and that I will not use the systems for personal or recreational use.
- I will not use any school server/computer/laptop/tablet/handheld device/cloud service for storing my own documents, photos, videos, music etc., nor to access any non-school personal accounts (such as email, cloud services, social networks, audio and video accounts).
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials; if I need access to a filtered website for school related purposes, I will liaise with the ICT Network and Services Manager.
- Should I need any other software on a device, I will consult the ICT Network and Services Manager for advice.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will keep any portable devices that are under my responsibility locked away when I am away from them. I will not take these devices offsite unless I have permission from my Head of Department/Line Manager, in which case I will sign it out and then sign it back in on return. I will remove any unneeded photos/videos before taking the device offsite.
- I understand that any issued equipment, such as laptops are only for me to use for school related purposes.
- I will take responsibility for any school equipment issued to me. This includes protection from both theft of the information and the device itself. This includes not leaving it in an unattended vehicle.
- I understand that the school will check my use of the ICT systems, work email, and other digital communications.
- I will at once report any damage or faults involving equipment or software, however this may have happened.
- I am aware that the use of computer systems without permission or for inappropriate purposes could be a criminal offence under the Computer Misuse Act 1990.

Personal Devices

- I will only use my own personal devices (e.g. phones, tablets, laptops, PDAs) in areas where no pupils will be present (this includes school trips)
- I will not have them on my person during the school day -unless moving from class / public area to office/staff room etc

- I will not connect my personal devices to any school equipment including the school's wireless network (Wi-Fi).
- I will follow the rules set out in this agreement in the same way as if I was using school equipment.
- I will take responsibility to ensure that my own devices are free from malware (Malicious software) including, but not limited to viruses and spyware.
- If staff have any wearable technology (such as smartwatches) and they have a camera, then these must not wear or take these into the bathroom areas.

Communications

- I will only use official school methods (School Email, Home school diary, School Phone, School headed Letter, School Parent messaging system) for communication relating to school.
- I will only use my school email account for emails relating to school activity; I will not use any personal email account nor give my personal email address to school based contacts, such as other professionals from different settings, pupils, and family members. There may occasionally be exceptional circumstances and these need to be agreed by the Head teacher.
- I will only use school telephones for calls relating to school activity; I will not use any personal telephone nor give my personal number to school-based contacts, such as other professionals from different settings, pupils, and family members.
- I will only use the school's address for postal correspondence and deliveries relating to school activity; I will not use or give out my home address to school based contacts, such as other professionals from different settings, pupils, and family members.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Please see Code of Conduct
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment having viruses or other harmful programmes.
- I will not engage in any on-line activity that may compromise my professional responsibilities or which may bring other staff, the school, or Sandwell LA into disrepute.
- I will not put my job title or the school name on my social networking pages.
- I will not put any information on social networking sites relating to the school.
- I will not put any information on social networking sites that may cause embarrassment to the school or bring the school into disrepute.
- I will not friend/follow/add/contact or access social networking pages of a pupil at the school, nor will I accept a request to friend/follow/add/contact a pupil.
- I will not friend/follow/add/contact or access social networking pages of parents or families of pupils or past pupils of the school, unless you are related, colleagues or you knew the person prior to the pupil starting the school. If this is the case, I will inform the designated safeguarding lead.

Data Protection and School User Accounts

- I understand that all routine school information should be treated as OFFICIAL, a subset of which may use the OFFICIAL-SENSITIVE caveat.
- I will only transport, hold, show, or share OFFICIAL information about myself or others, as outlined in the School's Data Protection Policy. Where I need to transfer OFFICIAL information outside the secure school network, I will encrypt the information.
- I will keep any staff or pupil's OFFICIAL information to which I have access private and confidential, except when the law or school policy needs me to show such information to an authority.
- I will not save any files that hold OFFICIAL information to the hard drives of any computer/laptop nor to the storage area of any tablet or handheld device; I will store such files on the school server/cloud service. I may use an approved (FIPS 140-2 certified) encrypted USB flash drive (with a secure password) if I need to transfer any files between devices, but I will not use this as a permanent data store. If a flash drive is damaged, faulty, or no longer needed, I will take this to the ICT Network and Services Manager.
- I will not use any unencrypted removable media for OFFICIAL information.
- Where technology does not allow encryption of data e.g. digital cameras and audio tapes, I will use a duty of care principle until I can move it to a secure location.

- I will make sure I have the authority, including the legal power to release any OFFICIAL information.
- I will never access any OFFICIAL information unless I have a need to do so as part of my job.
- I will never give out any OFFICIAL information via the telephone or in any other way unless I am sure who I am giving it to, that I protect it whilst in 'transit' and I have verified the entitlement of the recipient to receive it.
- I will only select photos/videos for the school website if they are suitable and, if they include children, I have written permission from the parents.
- I understand the importance of regularly backing up my work.
- I will not allow anyone to use a computer using my account; I will not tell others my username or password, nor will I try to use any other person's username and password.
- I will ensure that all my passwords meet the complexity requirements.
- I will log off or lock the screen when leaving a computer.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- If there is a breach of any data on any device, I will report it to ICT Network and Services Manager, Head Teacher, or Designated Safeguarding Lead.
- I am aware that there are data retention guidelines that I must abide by if I am the owner of original school / personal / sensitive data.

Inappropriate Material

- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will at once report any incident I become aware of relating to illegal, inappropriate, or harmful material to the ICT Network and Services Manager, Head Teacher, or Designated Safeguarding Lead.
- If I am unsure about steps needed to keep information safe I will seek clarification from the ICT Network and Services Manager.

Copyright

- I will ensure that I have permission to use the original work of others in my own work.
- I will not use any of my personal audio or video streaming accounts in school or on any school equipment, nor will I download anything from these to then use in school or on any school equipment.
- It is my responsibility to understand and follow current copyright legislation

---

Declaration

I have read and understand the Orchard School Acceptable Use of Technology guidelines and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: **Designation:**

Signed: **Date**

Please return to Barbara Ackerley

APPENDIX 2

Acceptable Use of The Orchard School's Technology Agreement for Parents

Name of child:

_____

If my child is provided with a School laptop/tablet/handheld device to use at home I will:

- Supervise my child when they are using the device and only use it for educational purposes.
- Not attempt to access any inappropriate websites.
- Only use the software installed in the device and not attempt to download any Apps myself.
- Not store any images on the device.
- Report any faults with the device to my child's teacher promptly.
- Use the device responsibly and return it to school promptly on the required date.

_____

Declaration

I have read and understand the above and agree to use the school I pad within these guidelines.

Name: **Relationship to child (Parent/ Guardian) Other**

Signed: **Date:**

Please return to your child's teacher

APPENDIX 3

The Orchard School Data Security Agreement

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-

Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the school.

Staff should only save sensitive data in the following secure formats:-

1. On the school server or the school cloud service
2. On the encrypted USB memory stick provided (but not as a permeant store)

This ensures that no legal action can be taken for lost data.

If you lose your encrypted memory stick or are unable to open it because of a password error, you must inform the ICT Network and Services Manager without delay. It is imperative that you do not share or write down your password. It is your responsibility to keep the data from your memory stick regularly backed up in another secure format as detailed above. Sensitive data should not be sent via email to external agencies, third party agencies or those no employed by the school unless it is encrypted/password protected.

Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

Declaration

I understand the Orchard School data security procedures and agree to follow these.

Name: **Designation:**

Signed: **Date**

Please return to Barbara Ackerley

APPENDIX 4

Online safety incident report log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident	Received and details of action taken