Oaklands Junior School

E-SAFETY POLICY

Statement

The Governing Body recognises the importance of having a policy and procedure in place for E-Safety.

The Governing Body has agreed to adopt the Wokingham Borough Council model policy and procedure for E-Safety, a copy of which is attached.

Review

The Curriculum committee will review the policy every year. Any alterations to the content notified by Wokingham Borough Council will be effective immediately.

Approved by the Curriculum Committee:	**June 2018**
Ratified by the Full Governing Body:	**July 2018**
To be reviewed:	**Spring 2021**

Related Documents:

- Safeguarding Policy
- Data Protection Policy
- Computing Policy
- Disciplinary Policy
- Whistleblowing Policy
- Best Value Policy
- Staff Handbook
- DfE Teachers' Standards https://www.gov.uk/government/publications/teachers-standards
- DfE statutory guidance on Keeping Children Safe in Education

Oaklands Junior School
E-Safety Policy

Appendix to the Data Protection Policy

This policy has been adapted from the Wokingham LA 'All in One' e-Safety Policy version 3.8.1 November 2015) provided by Philip Mann.

Introduction

The purpose of this policy is to address the full scope of current risks in relation to ICT use at Oaklands Junior School, including aspects of data security, password security and encryption.

1 Roles and Responsibilities

1.1 Governors

Governors are responsible for the approval of the e-Safety Policy (including Acceptable Use agreements), ensuring that it is implemented and reviewing its effectiveness. Governors will undertake the following regular activities:

- Meetings with the e-Safety Co-ordinator
- Monitoring of e-safety incident logs
- Reporting to relevant governor committees
- Keeping up to date with school e-safety matters.

1.2 Headteacher

The Headteacher is responsible for ensuring the safety, including e-safety, of members of the school community. The day to day responsibility for e-safety may be delegated to the e-Safety Co-ordinator , Computing Subject Leader or another appropriate member of staff. However, the Headteacher will ensure the following:

- Staff with e-safety responsibilities receive suitable and regular training, enabling them to carry out their e-safety roles and to train other colleagues as necessary
- The Senior Leadership Team (SLT) receives regular monitoring reports
- There is a clear procedure to be followed in the event of a serious e-safety allegation being made against a member of staff.

1.3 E-Safety Co-ordinator

The e-Safety Co-ordinator has day to day responsibility for e-safety issues and takes a leading role in establishing and reviewing the school e-Safety Policy and associated documents. The e-Safety Co-ordinator will also:

- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provide materials and advice for integrating e-safety within schemes of work and check that e-safety is taught on a regular basis
- Liaise with the local authority
- Liaise with the school's technical staff
- Ensure that e-safety incidents are reported and logged and used to inform future e-safety developments
- Report to the governors and meet with them as required
- Report regularly to the SMT.

- Report to DPO – see Data Protection Policy

1.4 ICT Technician

The ICT Technician, will, in co-operation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- The ICT infrastructure is secure and protected from misuse or malicious attack
- The school meets the e-safety technical requirements outlined in any relevant local authority e-safety policy/guidance
- Users may only access the school's network(s) through a properly enforced password protection policy -Please read the link here https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry
- The school's filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person. Filtering is provided by SEGfL
- E-safety technical information is kept up to date, applied as necessary and passed on to others where relevant
- Use of the network and learning platform is regularly monitored and any misuse/attempted misuse reported to the e-Safety Co-ordinator or designated person for investigation and action.
- Appropriate steps are taken to protect personal information and secure data on all devices and removable media
- For approved staff provide secure access to the school network from home where necessary using VPN or equivalent technologies.

1.5 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current e-safety matters and the school e-Safety Policy and practices
- They have read and understood the school's Staff Information Systems Code of Conduct (*Appendix 1*) and signed to indicate agreement
- They report any suspected misuse or problem to the e-Safety Co-ordinator for investigation and action
- Digital communications with pupils (e-mail/learning platform/voice) should be on a professional level and only carried out using approved school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school's e-Safety and Acceptable Use Policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras (including cameras within mobile phones etc.) and handheld devices and that they monitor their use and implement school policies with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.

1.6 Designated Safeguarding Lead (DSL)

The DSL should be trained in e-safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying.

1.7 Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk. SMT should be informed where school policies may require updating.

[See *'Appendix 2 – School and the Data Protection Act'* for further information]

2 Reviewing, Reporting and Sanctions

2.1 Review

- This policy will be reviewed and updated annually in the Spring term by the Curriculum committee, or sooner if necessary.
- The school will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

2.2 Acceptable Use Agreements

- All users of the school computers will sign the appropriate Acceptable Use agreements. This includes all staff and pupils.
- Parents will be asked to sign the Responsible Internet Use Form *(Appendix 10 / 10A)* on behalf of their children to show agreement with and support for the school's policy.
- All users will be expected to re-sign agreements on a regular basis.

2.3 Reporting

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.

  [See *'Appendix 3 – Course of action if inappropriate content is found'* for further information]

2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

2.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

3 Communications & Communication Technologies

3.1 Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school.
- Where mobile phones are allowed in school they may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Pupils will not be allowed to bring in games devices, particularly those which allow *ad hoc* networks to be established or photographs to be taken.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call. They may not use mobile phone cameras whilst on school premises.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.
- Emerging technologies, eg smart watches will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.2 E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail and/ or messaging accounts will be monitored.
- Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils may only use approved e-mail or message accounts on the school system.
- Pupils should immediately tell a staff member if they receive an offensive e-mail or message.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff before sending.
- Information of a sensitive nature should not be sent by unencrypted e-mail.

3.3 Social networking

For the purpose of this policy, social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, blogs, chat rooms, online gaming, YouTube, Instant Messenger, Skype, Whats App, Instagram, Second Life, Club Penguin, Tinder, Poptropica, Habbo, Stardoll, etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.

- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
- The use of social networking 'tools', e.g. blogs, wikis, messaging, etc., within a school learning platform is both acceptable and to be encouraged.

  [See *'Appendix 4 – Social Networking Guidance'* for further information]

3.4 Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- 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.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- All pupils using the internet and associated communication technologies will be made aware of the school's e-Safety Guidelines. These should be posted near to the computer systems.
- Pupils will receive guidance in responsible and safe use on a regular basis.

3.5 Digital and video images

Parents, staff and pupils may record images of pupils at school under the following conditions:

- All staff digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny by managers if required
- Images of pupils must be stored securely and deleted when no longer required. Images that have been retained as part of the historical record of school will be stored securely
- Published photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained when the pupil is first admitted to the school before photographs of pupils are published on the school website (*see Appendix 5 for parental consent form) Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.*
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Images of pupils must be stored securely and deleted when no longer required
- Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The image should then be deleted from the temporary storage location.
- No images of pupils should be recorded
  - in toilets or wash areas
  - whilst pupils are getting changed
  - in the medical room

The only exceptions to this rule would be if images are recorded to illustrate a particular point for display (e.g. how to wash hands). In this case the Headteacher must be informed before this activity is undertaken.

- Where volunteers are supporting school staff, they should abide by the same rules as school staff as far as is reasonable.
- Parents may record images at "public events" such as assemblies, school plays or sporting activities, but they may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking or other websites that are accessible by the general public.
- Although the school will make reasonable efforts to safeguard the images of pupils, parents should be made aware that at some types of events involving multiple schools, it is not always strictly enforce image guidelines. The school cannot therefore be accountable for the use of images taken by parents or members of the public at events.

3.6 Learning platform and/or website

- The school learning platform and/or website should include the school address, school e-mail, telephone and fax number including any emergency contact details.
- The school learning platform and/or website should be used to provide information and guidance to parents concerning e-safety policies and practice.
- Staff or pupils' home information should not be published.
- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing.

4 Infrastructure and Security

4.1 Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School ICT technical staff may monitor and record the activity of users on the school ICT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician/Network Manager.
- Access to the school ICT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- The 'Administrator' passwords for the school ICT system, used by the ICT Technician are stored in the school safe.

4.2 Passwords

All staff are provided with an individual password to access the school network. Pupils may have a group password or individual passwords for accessing the network. All users will have an individual log on to the learning platform and/or secure areas of the website. All staff laptops have a boot up password and this must not be shared.

Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- No individual should tell another individual their password
- No individual should log on using another individual’s password, unless they are a member of staff logging on as a pupil
- Once a computer has been used, users must remember to log off so that others cannot access their information
- Users leaving a computer temporarily should lock the screen (Ctrl/Alt/Del and choose Lock This Computer option)
- In the event that a password becomes insecure then it should be changed immediately.

  [See *‘Appendix 6 – Password guidance’* for further information]

4.3 Filtering

The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

- Changes to network filtering should be approved by the ICT Technician.
- Any filtering issues should be reported immediately to the ISP and/or SEGfL.

4.4 Virus protection

- All computer systems, including staff laptops/devices, are protected by an antivirus product which is administered centrally and automatically updated.
- The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case only dependable sources should be used.

4.5 Staff laptops/devices

The following security measures should be taken with staff laptop/devices:

- Laptops should be secured to the cable lock when in the classroom
- Laptops/devices must be out of view and preferably locked away overnight whether at school or home
- Laptops/devices should never be left in a parked car, even in the boot
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.
- Tablets should be kept in a lockable storage when the teacher is not in the classroom (not yet available)

  [See *Appendix 1)*

4.6 Personal and sensitive data

- All users are responsible for only accessing, altering and deleting their own personal or team files. They must not access, alter or delete files of another user or team without permission.
- Sensitive data is any data which links a child's name to a particular item of information and:
  - must be encrypted on laptops/devices, memory sticks, CDs and any other removable media;
  - should not be e-mailed between staff;
  - should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.
- Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present. Sensitive documents that require printing should be retained and only printed out with the owner's print code.
- There must be clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.

  [See *'Appendix 7 – Sensitive and Non-Sensitive Data'* for further information]

4.7 Electronic Devices- search and deletion

Schools have the power to search pupils for items "banned under school rules" and the power to "delete data"on seized electronic devices.

- Electronic devices include smart phones and other devices which take photographs or link to the internet.
- The Headteacher, Designated Safeguarding Lead, or SLT may examine and/or delete data on electronic devices
- A pupil and/ or his/ her belongings will be searched if there is good reason to suppose that a banned school devise is present

- Data will be deleted from the device, with a copy kept in the secure central location as evidence
- Incidents will be reported to the e-safety co-ordinator and if appropriate the CPO

4.8 Loading/installing software

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- Only authorised persons, such as the ICT Technician, may load software onto the school system or individual computers.
- Where staff are authorised to download software to their own laptops/devices, they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

4.9 Backup and disaster recovery

The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:

- The use of a remote location for backup of key school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system
- No data should be stored on the C drive of any curriculum computer as it is not backed up automatically to the school servers
- Staff are responsible for backing up their own data stored on the C drive of any teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup
- The school has a whole school ICT disaster recovery plan which would take effect when severe disturbance to the school's ICT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised, including who would be involved in the process and how it would be accomplished.

5 E-Safety Education

5.1 Learning and teaching for pupils

- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key e-safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities (see Appendix 8).
- Rules for the use of computers should be displayed in all rooms and displayed next to fixed site computers (*see Appendix 9*).

5.2 Staff training

- Staff will be kept up to date through regular e-safety training.
- Staff should always act as good role models in their use of ICT, the internet and mobile devices.

5.3 Parental support

The support of, and partnership with, parents should be encouraged. This is likely to include the following:

- Awareness of the school's policies regarding e-safety and internet use; and where appropriate being asked to sign to indicate agreement *(see Appendices 10 and 10A)*
- Practical demonstrations and training
- Advice and guidance on areas such as:
    - filtering systems
    - educational and leisure activities
    - suggestions for safe internet use at home.

Appendix 1 – Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are the school's property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely, this includes laptops, discs, memory sticks, photocards etc.
- I will report any incidents of concern regarding children's safety to the School E-Safety Co-ordinator or the Child Protection Leader and the Headteacher.
- I will ensure that any electronic communications with pupils are compatible with my professional rôle.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

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

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ……………………………….. Capitals: ……………………………….. Date: …………...

Accepted for school: ……………………………………. Capitals: ……………………………….

Appendix 2 – School and the Data Protection Act

The Seventh Principle of the Data Protection Act (1998) states that:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

This means that schools must have appropriate security to prevent the personal data held (e.g. for staff, pupils and parents) being accidentally or deliberately compromised.

The implications of this for the school will be the need to:

- Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.
- Be clear about who is responsible for ensuring information security.
- Ensure that the school has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.
- Respond to any breach of security swiftly and effectively.

Failure to comply with the Act could result in loss of reputation or even legal proceedings.

Further guidance may be found at www.ICO.gov.uk

Appendix 3 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or in any way disturbing) the user should:
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
    - Ensure the well-being of the pupil.
    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the e-Safety Co-ordinator.
- The e-Safety Co-ordinator will then:
    - Log the incident and take any appropriate action, including the Child Protection Officer and ICT Technician as necessary.
    - The ICT Technician can ban/block websites and web content within minutes of the incident occurring.
    - Where necessary, the ICT Technician will report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

Appendix 4 – Social networking guidelines

Specific guidelines relating to staff use of social networking are best arrived at through discussion to both clarify and agree exactly what should be applicable. Aspects will also be applicable to those associated with the school, e.g. governors and parent helpers.

The following areas should be included in any policy:

Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a ‘private’ online space.

Access to social networking sites

- Social networking sites should not be used or accessed during school working hours.
- Staff may not use school equipment to access social networking sites.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make ‘official’ use of social networking sites this should only be by authorised individuals.

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be ‘friends’ with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents simply because they teach their children.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

Additional considerations

Thought should be given to what the implications of this policy will be for the different groupings within the staff employed at the school, e.g.

- Teacher
- Teaching assistant
- Other support staff, e.g. bursar, site manager, lunchtime supervisors, office staff, cleaners
- Outside agency staff, e.g. sports coaches, music tutors, etc.

Appendix 5 – Parental Photo Consent Form

Oaklands Junior School

Photo Consent Form

Name of Child: ____ Class: _____________

Name of Parent/Guardian: ____

We take a lot of photographs of the children at our school. These may be used in school displays, community displays, in printed publications or on our school website. **It is our policy to allow parents/carers to take photographs/video at school events on the understanding that they are for personal use only and will not be distributed anywhere e.g. Social networking sites such as Facebook. This includes photographs of staff.** We may also be visited, or attend events that are covered by the media. If photographs are taken for local or national publications, pupil's names will not be published without written parental permission.

To comply with the Data Protection Act 2018, we need your permission in order to use images of your child. We have strict conditions of use:

1. We will not use the personal details or names (i.e. first name or surname) of any child in a photographic image on our website.
2. We will not include personal addresses, e-mail addresses or telephone numbers of any child in a photographic image on display, in printed material or on our website.
3. We may include pictures of pupils and staff that have been drawn by the pupils.
4. We may use group or class photographs or footage with very general labels, such as “a science lesson” or “making Christmas decorations”. They may be stored for extended periods.
5. We will only use images of children suitably dressed.

6. Photos will be deleted in line with the Data Protection Policy

Please answer the question below. To administer this efficiently, the permission needs to **'yes' to all or 'no' to all**.

May we, Oaklands Junior School, use your child's photograph and include your child in media events as described above? Please tick whichever is appropriate.

□ YES □ NO

I have read and understood the conditions of use.

Parent/Carer's Name ____________________________ Date ______________

Signature ____________________________

Appendix 6 – Password guidance

- Passwords should have strength of at least 12 where a letter is 1 and a number or punctuation mark is 2.
- Passwords must not be easily guessable by anyone and therefore should not include:
    - Names of family, friends, relations, pets etc.
    - Addresses or postcodes of same
    - Telephone numbers
    - Car registration numbers
    - Unadulterated whole words
- Try to use in a password:
    - A mixture of letters and numbers
    - Punctuation marks
    - At least 8 digits
- Possible ideas are
    - Choose a word which has o and i in and substitute 0 (zero) and 1, e.g. sn0wt1me.
    - Use the initial letters of a familiar phrase, song title etc. and substitute as above.
    - Use a text message abbreviation, e.g. CUL8R

Appendix 7 – Sensitive & Non-sensitive data

Sensitive data will include:

- SEND records such as Pupil Support Plans and Educational Health Care Plans (EHCP)
- Mark sheets and assessments
- Reports and Open Evening comments
- Personal data stored on the school’s Management Information System, e.g. SIMS
- Photographic or video material
- Name, address and contact information

Non-sensitive data thus includes:

- General teaching plans
- Curriculum materials
- General correspondence of a non-personal nature

Appendix 8

👍 I'm SMART with E-Safety!

S

Keep Safe – I always keep my full name, address, mobile phone number, e-mail address, password, school name and other's full names secret from people I don't know. This means people on the Internet cannot use this information to contact me or others. I never send this information, or my or other's photo, to anyone without checking with a parent, carer or teacher first.

M

Don't Meet Up – I never arrange to meet an online friend, no matter how well I think I know them, unless I have permission from my parent or carer.

A

Accepting e-mails can be dangerous – I never open an e-mail or an attachment from someone I don't know, unless I have checked with a teacher, parent or carer first.

R

Reliable? – I know that people online might not be who they say they are. Online games, chat rooms, message boards and social networking sites are fun but they can be dangerous because I don't always know who I am talking to. I will also always be myself online and will not pretend to be anyone or anything that I am not.

T

Tell Someone – I will always tell an adult if something or someone makes me feel uncomfortable or worried. I understand that saying or writing nasty things about others using a computer or a mobile phone is called cyber bullying and is the same as bullying someone in the real world.

FOLLOW THE SMART E-SAFETY CODE WHEREVER YOU ARE! 👍

Appendix 9

The Oaklands SMART E-Safety Code

To keep safe when I am using OWL and the Internet:

- I will only log on with my own username and password and I will not use one that belongs to someone else.
- I will not tell anyone else my OWL password and I will always log off when I have finished.
- I will be sensible about what I put on my OWL homepage and other work.
- I will only search the web if an adult is in the same room as me.
- I will only use agreed websites when given permission by a teacher.
- I understand the copying text or images that belong to someone else may be illegal and will take care to respect and check copyright.
- I know that I shouldn’t send unkind messages to anyone.
- I will tell an adult if I find anything that upsets me on the internet.
- I will not visit chat rooms, chat rooms in online games, message boards and social networking sites (Facebook, Instagram etc) on the school site and in school time
- I know that my school can check the websites I have visited.
- I will not access my own email site on the school site.
- I will give memory sticks or CDs from home to the teacher or ICT Technician to be virus checked. I will use OWL to upload work from home.
- I follow the SMART code when using computers in school and at home.

Be a Safe Surfer and stay SMART!

Appendix 10 – Responsible Internet Use Letter and Form

OAKLANDS JUNIOR SCHOOL

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Oaklands Junior School provides supervised access to the Internet. We believe that the 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, sign and return the consent form so that your child may use the Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we take positive steps to deal with 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.

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.

Yours sincerely

Hazel West

Headteacher

Oaklands Junior School

Responsible Internet Use (Appendix 10A)

Please retain the SMART E-Safety Code at home and complete, sign and return this consent form to the school.

Pupil:	***Class:***
Pupil's Agreement: • I have read and understand the Oaklands Smart E-Safety Code • I will use the computer system and Internet in a responsible way and obey these rules at all times. • I know that I can only use the OWL if I agree with all these rules.	
Signed:	***Date:***
Parent's Consent for Internet Access and use of Oaklands Learning Platform (OWL LIFE): • I have read and understood the school rules for the Oaklands SMART E-Safety Code 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:	