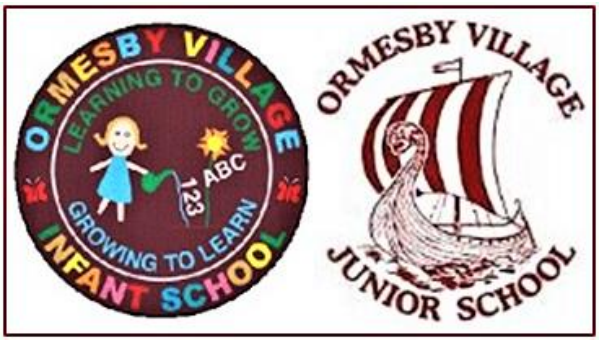

Ormesby Village Infant & Junior Schools Federation

E-Safety Policy 2023

Updated 23rd May 2023

Ormesby Village Infant & Junior Schools Federation E-Safety Policy

Writing and reviewing the E-safety policy

This policy relates to other policies including those for ICT, bullying and for child protection.

- The school will identify a member of staff who has an overview of E-safety, this would usually be the Designated Safeguarding Lead (DSL).
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-safety Policy and its implementation will be reviewed annually

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the curriculum and a necessary tool for staff and pupils.

- The school Internet access is provided by Updata and includes filtering appropriate to the age of pupils in a UK KS1-2 Infant & Junior School.

  Updata: 7 Bell Yard, London, WC2A 2JR.
  Sales Email: TA@updata.co.uk
  Technical Support Email: TAsupport@updata.co.uk

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

- Pupils will be educated in the effective use of the Internet

- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.

- Pupils will be taught using a computer programme specifically designed to raise awareness of E-Safety through secure online gaming platforms.

- Pupils will be taught be taught about extremist and terrorist content and taught how best to protect themselves from any such content.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly – by Jonathan Lee every six months

- Virus protection will be updated regularly – Automatic subscription service paid for versions that update daily/weekly on every school Desktop and Laptop device. Regular scheduled virus scans of devices will be configured by IT Support.

- Security strategies will be discussed with the Local Authority and IT Support (Jonathan Lee) once every academic Year

  Jonathan Lee from Netcentral Solutions Ltd - Unit 3G Snetterton Business Park Harling Road, Snetterton, Norfolk, NR16 2JU

E-mail

- Pupils may only use approved e-mail accounts, that refers to any account using the ormesbyinfant.school or ormesbyjunior.school domain name.

- Pupils must immediately tell a teacher if they receive offensive e-mail

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school will consider how e-mails from pupils to external bodies are presented and controlled.

- The forwarding of chain letters is not permitted.

Google Drive/Microsoft Onedrive and online storage

- Google Drive/ MS OneDrive and all online cloud storage must only be used for the use the school. You may create a Folder called 'Personal' however this should be used for work related personal files and not personal pictures or non-work related storage.

- It is not permitted to share any pictures/files including lesson plans and strategic planning with any other person or organisation outside of the OVSF without the consent of the Headteacher or Governing board.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published without prior consent (Governor details will be published, however all contact will be made through the school office).

- Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children. Where full face photos are required permission will be sought from the parents before publication.

- Pupils' full names will be avoided on the website or public areas of the learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

- Blanket permission is obtained at the start of the school year to cover the use of photographs on the school website.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords/privacy settings.

- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

- Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

- Staff will not contact parents regarding any school matters through any social media.

- Pupils, parents and staff will be advised on the safe use of social network spaces

- Pupils will be advised to use nicknames and avatars when using social networking sites.

- Staff should consider not using their 'Real' names on Social Media websites if they are in direct contact with pupils. (eg. Form Teacher).

- Staff members social network profiles should be marked as Private, and content should only be shared with 'Friends only' and not the general public. It is encouraged that public posts don't contain personal profile pictures of the staff member. Social Network Profiles such as Facebook, Instagram, Twitter should be 'locked down' as much as possible in relation to their content.

  For example:

  If the Profile contains content that is regarding a personal hobby or business, then this can be made public as long as the image is relevant to the post and doesn't offend or put the member of staff in danger or risk other staff or pupils attending the school.
  If the Profile contains personal holiday pictures and close up images of a member of Staff and their family, then this should be marked as 'Friends only' and the profile can't be contacted or found on the Internet or Social media app other than by authorised App 'Friends'. (Not - Friends of Friends)

Managing filtering

- The school will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved. Net Sweeper (Securly if system is altered) administrator rights are limited to the Headteacher and Net Central – overall responsibility for filtering lies with the Headteacher.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher or IT Technician.

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- The Headteacher will oversee any videoconferencing communications using the relevant approved software such as Skype, Google Meet, MS Teams and Zoom with only an authorised school account.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- Video-conferencing will be supervised at all times.

Managing emerging technologies

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

Other devices

- Our school is a **mobile phone free site** between the hours of 8.00am and 4.30pm. There are specified 'mobile zones' where phones may be used by staff if needed. Mobile phones should not be used in classrooms during the set hours without prior consent from the Headteacher.

- Taking photographs at any time without the subject's consent will be discouraged.

- The sending of abusive, offensive or inappropriate material is forbidden.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use. Internet access through these devices is not allowed. Certified Age-restricted games will only be used on the games machine in relation to the pupils' ages using the devices. *(For example – Minecraft is age 7+)*

- Staff should not share personal telephone numbers with pupils and parents.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR policy of 2018.

- All staff work laptops, must all be encrypted with Bit-locker or an Equivalent software with a minimum 128bit encryption. (256bit recommended with TPM chip). This is to ensure there is no data loss in the event of loss or theft of the item. Recovery Passwords and Keys should be kept in a secure location in paper format.

- All staff work laptops must all have a password with at least 8 characters, containing 1 upper and lower character, and 1 number. This password must be updated every 90 days.

- All USB sticks/external hard drives and Memory storage devices used for holding School data (except camera storage) must be encrypted in line with all staff laptops. Teaching staff have all got encrypted memory sticks. Any new USB storage device must be encrypted before being used. If a memory stick is lost please inform the Headteacher within 24hours.

- Any email accounts linked to personal mobile devices should be password protected with a minimum 6 digit passcode. If a mobile device is lost, please inform the Headteacher if an email account has been linked to it within 24hours.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff E-Safety Policy and Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents, carers and children will be asked to sign and return a consent form.
- Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
  The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead and dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Social networking

Social media is the term commonly used for websites which allow people to interact with each other in some way (social networking) – by sharing information, opinions, knowledge and interests. Social media is part of many people's day to day lives. The following information has been put together for the benefit of employees to help them understand what may be deemed appropriate or inappropriate both inside and outside of work.

Social media is another form of communication and is not necessarily private. Employees should consider if it would not be said to a current or future colleague or parent, pupil or manager then it should not be published on a social networking site, whether this is a school managed site or a personal one.
Online conduct should be as exemplary as offline conduct. Employees and volunteers must have regard to the fact that anything that is said on the internet could at some point be made public.

The school recognises that social networking sites, websites and blogs provide a useful tool for communication and learning and are accessed widely. However the safeguarding of pupils and employees is of paramount importance, adults should lead by example and set standards of behaviour. Therefore:

1.1. Safeguarding of pupils and employees is the responsibility of all employees and this should also be taken into consideration when using personal social networking sites inside and outside of the school. Employees should not link their own personal social networking sites to anything related to the school.

1.2. Employees are advised not to communicate with pupils or accept pupils as friends on social network sites using their personal systems and equipment. Where a member of staff is related to a pupil the school should be made aware, if they are not already, and consideration given to whether any safeguards need to be put in place. Employees should also consider carefully the implications of befriending parents, carers or ex-pupils as contacts on social networking sites.

1.3. Any communication with pupils should take place within clear and explicit boundaries

1.4. If employees use personal social networking sites they should not publish specific and detailed public thoughts or post anything that could bring the school into disrepute.

1.5. Employees must not place inappropriate photographs on any social network space and must ensure that background detail (e.g. house number, street name, school) cannot identify personal/employment details about them.

1.6. Official blogs, sites or wikis must be password protected and overseen and sanctioned by the school.

1.7. Contact should only be made with pupils for professional reasons via professional spaces set up and run by the school. If professional spaces are set up steps should be taken to ensure the users of the space are not put at risk e.g. privacy settings, data protection and data security. Permission should be sought from the Headteacher and the parents/guardians of pupils to communicate in this way.

1.8. Employees are advised not to run social network spaces for pupil use on a personal basis. If social networking is used for supporting pupils with coursework, professional spaces should be created by employees and pupils as in paragraph 6.7 above.

1.9. Employees are advised not to use or access the social networking sites of pupils, without due reason e.g. safeguarding purposes. However, this may not be possible to achieve if the situation in 6.2 applies.

1.10. If an employee feels they are a victim of cyberbullying they should report it via the appropriate channels, please see below.

If employees or managers need to seek advice about inappropriate use they can contact the Online Safety Helpline (email: helpline@saferinternet.org.uk or call 0844 3814772). However, employees and managers should not bypass the school's safeguarding procedures.

2. The consequences of improper/unacceptable use

2.1. The Headteacher can exercise their right to monitor the use of the school's information systems and internet access. This includes the right to intercept email and the right to delete inappropriate materials where they believe 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 text, imagery or sound.

2.2. Employees must be aware that improper or unacceptable use of the internet or email systems could result in legal proceedings and the use of the school's Disciplinary Procedure. Sanctions will depend upon the gravity of misuse and could result in summary dismissal in some cases.

This policy was approved by the Governors on_____.

This policy will be reviewed annually unless government legislation requires an earlier update.

Signed: ……. (Headteacher)

Signed: …….. (Chair of Governors)

Staff, Governor and Visitor – ICT Code of Conduct / Acceptable Use

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This code of conduct is provided to ensure that all users are aware of their responsibilities when using any form of ICT provided by or directed by Norfolk County Council. All such users will be issued with this code of conduct. Any concerns or clarification should be discussed with the Headteacher.

- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, laptops and tablets

- All staff understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.

- All staff, Governors and visitors will abide by the rules on the use of mobile phones within school. These rules restrict the use of mobile phones between the hours of 8.00am and 4.30pm

- All staff, Governors and visitors will not disclose any passwords provided to them by the school or other related authorities.

- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username

- Staff, Governors and visitors will not install any hardware or software on any school owned device without the permission of the Headteacher or the school's IT Technician.

- All staff, Governors and visitors understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to their Headteacher in line with any disciplinary procedures. This relates to all school owned devices, including laptops provided by the school.

- All staff, Governors and visitors will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Body.

- All staff, Governors and visitors will ensure that all their school generated electronic communications are appropriate and compatible with their role.

- All staff, Governors and visitors will report any content of an inappropriate, sexual, extremist or terrorist nature to DSL as a cause for concern immediately.

- All staff, Governors and visitors will ensure that all data is kept secure and is used appropriately as authorised by the Headteacher or Governing Body. If in doubt they will seek clarification. This includes taking data off site or sharing with other organisations outside of OVSF (Google Drive shares)

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images will only be taken, stored and used for purposes in line with school policy. Images will only be taken on school cameras and will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Headteacher.

- All staff, Governors and visitors will refrain from discussing school issues, or posting anything that could be classed as defamatory or offensive related to school, on social networking sites.

- All staff, Governors and visitors will comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Senior Designated Professional or Headteacher in line with the school's Safeguarding Policy.

I acknowledge that I have received a copy of the ICT Code of Conduct.

Full name :……(printed)

Job title :……

Signature:……**Date:**……

E-safety agreement form: parents

Parent / guardian name:……

Pupil name: ……

Pupil's class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest information is available at the School Office, and that further advice about safe use of the Internet can be found through the Headteacher.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent's signature:……

Date:……..

E-Safety Check List

The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
Has the school got an E-safety Policy that allies with Norfolk guidance?	**Y/N**
When was the policy updated/reviewed?	
The school E-safety policy was agreed by governors on:	
How is the policy made available for staff?:	
How is the policy made available for parents/carers?:	
Has E-safety training been provided within the last year for both pupils and staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y/N**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Y/N**
Are all pupils aware of the School's E-safety Rules?	**Y/N**
Are E-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School E-safety Rules?	**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. Regional Broadband Consortium, NEN Network, EXA, Updata)?	**Y/N**
Have E-safety materials from CEOP been obtained?	**Y/N**
Is personal data collected, stored and used according to the principles of GDPR 2018?	**Y/N**
Where appropriate, have teaching and/or technical members of staff attended training on the school's filtering system?	**Y/N**

Date:_____

Signed and checked by:_____

Acceptable Use Policy – Technology Rules for Children

OUR TECHNOLOGY RULES

Technology is all around us and we use it every day. Please read these internet rules with your parents so that you know how to stay safe whilst at school. Once you have read them you need to sign at the bottom and return this form to your teacher.

Always report anything that you are worried about on the internet to a teacher and never look at the wrong sort of websites on purpose.

We only ever use kind words and images. Never send anyone nasty or offensive emails or messages.

Always ask before you look at other peoples files and never go on the internet without telling a teacher.

Only use the software on the computers, never try to install your own and always ask a teacher before using a memory stick from home.

We never give out personal information such as phone numbers and addresses and never arrange to meet someone that you meet on the net!

School computers are only for school work, we never play games without permission.

Computers are very fragile. Always take care of school equipment and let a teacher know if something is broken.

Children who do not stick to these rules will have their computer access limited at school. This includes children who cyber-bully outside of school.

I have read the school technology rules and I promise to use school computers in the right way.

Name: _____ Class: _____

Signed: _____ Date: _____