

Toftwood Infant School
School Lane
Toftwood
Dereham
Norfolk
NR19 1LS

01362 692612

admin@toftwood.norfolk.sch.uk



Toftwood Junior School
Westfield Road
Toftwood
Dereham
Norfolk
NR19 1JB

01362 694919

reception@toftwood-jun.co.uk

Website: www.toftwood.norfolk.sch.uk
Toftwood Infant and Junior School Federation
Executive Headteacher - Mrs Joanna Pedlow

Online Safety Policy

1. Statement of intent

At our Federation we understand that computer technologies are an essential resource for supporting teaching and learning and preparing children for the future. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst we recognise the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use to ensure online safety.

We have created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils, staff and visitors to the Federation.

We are committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

This policy has been reviewed in line with the document Keeping Children Safe in Education, 2018 which explicitly mentions online safety. This document is available online at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education_3_September_2018_14.09.18.pdf

2. Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- **The Regulation of Investigatory Powers Act 2000**
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

2.1. This policy also has regard to the following statutory guidance:

- DfE (2018) 'Keeping Children Safe in Education'

3. Use of the internet

3.1. Our Federation understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

3.2. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

3.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

4. Roles and responsibilities

4.1. It is the responsibility of all staff and governors to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the schools, and to deal with incidents of such as a priority by following the procedures outlined in the Safeguarding and Child Protection Policy.

4.2. The online safety officer, (Amanda Bell), is responsible for ensuring the day-to-day online safety in our schools and managing any issues that may arise.

4.3. The Executive Headteacher is responsible for ensuring that the online safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

- 4.4. The online safety officer, and Computing subject leaders will work together, to ensure all online access is secure and that staff receive relevant training and provide relevant advice for members of staff on online safety.
- 4.5. The Executive Headteacher and SLT will ensure there is a system in place which monitors online safety in the schools, keeping in mind data protection requirements.
- 4.6. Online safety concerns are reported to the online safety officer, or another Designated Safeguarding Lead in line with procedures set out by the Safeguarding and Child Protection Policy. Online safety concern forms are stored with child protection records within a folder in a locked cabinet in line with the federation Safeguarding and Child Protection Policy.
- 4.7. All staff are made aware of reporting procedures in regular Safeguarding and Child Protection training, or as part of the induction process if they join the Federation during an academic year.
- 4.8. The online safety officer and SLT will regularly monitor the provision of online safety in the schools.
- 4.9. The Governors' policy is that no member of the Federation community should mention the school on social media sites. See social networking policy and code of conduct.
- 4.10. Cyber bullying incidents will be reported in accordance with the school policies.
- 4.11. The Governing Board monitor safeguarding and child protection procedures in school to ensure effectiveness of online safety provision, and handling of online safety concerns. In our Federation, the Governing Board has a Human Resources and Safeguarding Committee, and a designated Safeguarding link governor to ensure this can take place effectively. Confidential and anonymous safeguarding and child protection updates are provided for the full Governing Board on a regular basis to allow appropriate challenge and support of actions and procedures.
- 4.12. The Governing Board will evaluate and review this Online Safety Policy on an annual basis, taking into account the latest developments in ICT and available technologies and feedback from staff/pupils.
- 4.13. The Executive Headteacher will review and amend this policy with the online safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.
- 4.14. All staff are responsible for ensuring that online safety is an embedded part of the wider curriculum in federation, and safe internet access is promoted at all times.

- 4.15. All staff are responsible for ensuring they are up-to-date with current online safety issues, and this Online Safety Policy.
- 4.16. All staff and pupils will ensure they understand and adhere to our Acceptable Use Policy. Parents and carers sign and return the agreement to the Executive Headteacher as part of the admission forms.
- 4.17. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately, and are responsible for promoting online safety and safe use of all technology at home.
- 4.18. The Federation provides an annual Computing Workshop for Parents, which includes information about online safety to support safe internet use at home.
- 4.19. The schools share relevant computing and online safety information via the Federation website to enable parents and carers to promote safe internet use at home.
- 4.20. The Federation website contains an embedded link to report online safety concerns directly to CEOP which ensures the ability to report concerns within school and from home settings.
- 4.21. The SLT communicates with parents and carers with appropriate information to update them on current online safety issues and control measures.

5. Online safety control measures

5.1 Educating pupils:

- The teaching of online safety is established and taught as part of the curriculum to ensure pupils are aware of how to access and use the internet and other technology safely both inside and outside of school.
- Pupils are taught about the importance of online safety and are encouraged to be aware of the content they access online.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any concerning use of the internet and digital devices to safe adults within school.

5.2 Educating staff:

- All staff undergo online safety training as part of their safeguarding and child protection training and through regular safeguarding updates.
- All staff employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff are aware of which sites are deemed appropriate and inappropriate. High standards of online conduct are ensured through the governor Code of Conduct.

- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff receive an online safety briefing as part of their induction programme, ensuring they fully understand this Online Safety Policy.

6. Internet Access

- Internet access will be authorised once parents and pupils have returned the signed consent form as part of our Acceptable Use Policy which is also contained within the Admission Form.
- A record will be kept by the school offices of all pupils who have not been granted internet access.
- Effective filtering systems are in place to minimise potential risks to pupils through access to websites that may pose an online safety or wider child protection risk.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by two members of the SLT.
- All school systems will be protected by up-to-date virus software administered by the school's technical support provider.
- The master users' passwords will be available to the SLT for regular monitoring of activity as required. There are designated staff responsible for setting up passwords for staff.
- Staff are not able to use the Federation's internet for personal use on personal devices, but may be able access the internet on personal devices such as mobile telephones. Staff are permitted to use the internet for personal use outside of direct teaching times as long as they do this in line with the code of conduct and access only appropriate sites.
- Personal use will be monitored by the SLT for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only. This will be dealt with as a matter in line with the governor Code of Conduct for staff.

7. Email:

- Staff will be given Federation approved email accounts and should always use these accounts for any work related correspondence.
- Use of personal email to send and receive personal data or confidential information related to work is prohibited.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.
-

8. Social networking: Full details are provided in the Social Networking Policy

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by two SLT members as outlined above.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.

9. Published content on the school website and images:

- The Executive Deputy Headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate in conjunction with the Executive Headteacher .
- All contact details on the website will be the phone, email and address of the school. No personal contact details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and in line with school policy and parental permission.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school policies. Staff will not take images using their personal equipment.

10. Mobile devices and hand-held computers:

- Mobile devices, such as mobile telephones are not permitted to be used in class or in areas where children are present during school hours by pupils or members of staff or visitors.
- Staff are permitted to use hand-held computers which have been provided by the school though internet access will be monitored for any inappropriate use by the online safety officer and SLT when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices must not be used to take images or videos of pupils or staff.

11. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the Federation's ICT technical support providers.
- The SLT ensure that the filtering of websites and downloads is up-to-date and monitored.

12. Cyber bullying

- 12.1. For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

- 12.2. We recognise that both staff and pupils may experience cyber bullying and will commit to preventing any instances that could occur.
- 12.3. We will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- 12.4. We will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- 12.5. We have zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our policies.
- 12.6. The Executive Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their Local Authority of the action taken against a pupil.

13. Reporting misuse

Misuse by pupils:

- Misuse by pupils will be dealt with by staff in accordance with our behaviour policy.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will be referred to a member of the SLT who will decide upon the appropriate course of action.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding and Child Protection Policy and procedures.

14.

Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to a member of the SLT.
- The SLT will deal with such incidents in consultation with HR and may decide to take disciplinary action against the member of staff.
 - The SLT will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

This policy was reviewed and agreed in accordance with governing body procedures in February 2019.

Executive Headteacher.....

Chair of Governors

