



The Winterton Federation e-Safety Policy



e-Safety Co-ordinator – Adam Downs and Sheliza Goodall
Computing Co-ordinator – Adam Downs and Sheliza Goodall
e-Safety Governor – Cheryl Baxter
DSL – Cathy Logan and Dawn Lovatt

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. The Winterton Federation endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

Links to other policies and national guidance

The following Federation policies and procedures should also be referred to:

- Safeguarding and Child Protection Policy;
- Whistleblowing Policy;
- Behaviour Policy;
- Anti-bullying Policy;
- Mobile phone Policy;
- Social Media Policy;
- Data Protection Policy;
- Staff code of conduct.

The following local/national guidance should also be read in conjunction with this policy:

- PREVENT Strategy HM Government;
- MARS (Multi-Agency Resilience and Safeguarding board);
- Keeping Children Safe in Education DfE September 2019;
- Teaching Online Safety in Schools DfE June 2019;
- Working together to Safeguard Children;
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our schools but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We provide a curriculum which has e-Safety related lessons embedded throughout;
- We celebrate and promote e-Safety through a planned programme of assemblies, collective worship, and whole-school activities, including promoting Safer Internet Day each year;
- We discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials;
- Any internet use is carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas;



The Winterton Federation e-Safety Policy



- Pupils are taught how to use a range of age-appropriate online tools in a safe and effective way;
- We remind pupils about their responsibilities through an Acceptable Use Policy which every pupil signs and is displayed throughout each Federation school;
- Federation staff model safe and responsible behaviour in their own use of technology during lessons;
- We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area;
- When searching the internet for information, pupils are guided to use age-appropriate search engines. All use is monitored and pupils are reminded of what to do if they come across unsuitable content;
- Pupils are taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-bullying Policy;
- Pupils are made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff Training

Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the e-Safety Policy, the Federation's Acceptable Use Policy, e-security and reporting procedures;
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-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 e-Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access

- The Federation agrees on which users should and should not have internet access and the appropriate level of access and supervision they should receive;
- All users sign an Acceptable Use Policy provided by the Federation, appropriate to their age and type of access. Users are made aware that they must take responsibility for their use and behaviour whilst using the school ICT system and that such activity is monitored and checked;
- All pupils access the network using an individual username and a class password which the teacher supervises;
- All internet access is undertaken alongside a member of staff or, if working independently, a member of staff supervises at all times;
- Members of staff access the internet using an individual ID and password, which they keep secure. They ensure that they log out after each session and do not allow pupils to access the internet through their ID or password. They abide by the school AUP at all times.

Managing Filtering

- The Federation has the Nebula filtering system in place which is managed by the Federation and acs. Banned phrases and websites are identified;
- The Federation has a clearly defined procedure for reporting breaches of filtering. All staff and pupils are aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training/online safety lessons;
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co-ordinator immediately;



The Winterton Federation e-Safety Policy



- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety Co-ordinator. The Federation will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF), and the government's counter-terrorism government referral unit (CTIRU);
- Any amendments to the Federation filtering policy or block and allow lists are checked and assessed by the Executive Headteacher/e-Safety Co-ordinator prior to being released or blocked;
- The evaluation of online content materials is a part of teaching and learning in every subject and is viewed as a whole-school requirement across the curriculum.

E-Mail

- Staff and pupils only use approved email accounts allocated to them by the Federation and are aware that any use of the school email system is monitored and checked;
- Staff do not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers;
- Staff do not send emails to pupils;
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails;
- Irrespectively of how pupils or staff access their school email (from home or within school), Federation policies still apply;
- Chain messages are not permitted or forwarded on to other Federation owned email addresses.

Social Networking

- Staff do not post content or participate in any conversations which are detrimental to the image of the Federation. Doing so will result in disciplinary action or dismissal;
- Due to close connections to the local community, there is the expectation that staff maintain their professionalism, if their account has links to members of the community;
- School blogs or social media sites are password protected and run from the Federation website with approval from the Senior Leadership Team;
- For additional information, please see the Social Media Policy.

Pupils Publishing Content Online

- Pupils are not allowed to post or create content on sites unless the site has been approved by a member of the teaching staff;
- Pupils' full names are not used anywhere on the website, particularly in association with photographs and video;
- Written permission is obtained from the parents/carers before photographs and videos are published;
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment;
- Pupils and staff are not permitted to use personal, portable devices to store images/video/sound clips of pupils, unless prior permission is given by the Executive Headteacher.



The Winterton Federation e-Safety Policy



Mobile Phones and Devices

General use of personal devices

- Mobile phones and personally-owned devices are not used in any way during lessons or school time. They should be switched off or silent at all times;
- No images or videos are taken on mobile phones or personally owned devices, unless permission is given by the Executive Headteacher;
- In the case of school productions, parents/carers are not permitted to take pictures of their child in accordance with school protocols;
- The sending of abusive or inappropriate text, picture or video message is forbidden;
- For further information, please see the Mobile Phone policy.

Pupils' use of personal devices

- Pupils who bring a personal device, must leave their device in the school office.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm;
- disrupt teaching;
- break school rules;
- commit an offence;
- cause personal injury, or
- damage property.

Staff use of personal devices – all the guidelines are to be followed, unless authorisation is granted by a member of the Senior Leadership Team.

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity;
- Staff do not use personal devices such as mobile phones or cameras to take photos or videos of pupils and only use school provided equipment for this purpose;
- If a member of staff breaches the Federation's policy, then disciplinary action may be taken;
- Mobile phones and personally owned devices are switched off or switched to 'silent' mode, and mobile phones or devices are not used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.

CCTV

- The Federation uses CCTV in some areas of school property as a security measure;
- Cameras are only used in appropriate areas and there is clear signage indicating where it is in operation.



The Winterton Federation e-Safety Policy



General Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff take care to ensure the safety and security of personal data regarding all of the Federation population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

Personal and sensitive information is only sent by e mail when on a secure network. Personal data is only stored on secure devices.

In the event of a data breach, the Federation will notify the Federation's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

Authorising Internet access

- All staff read and sign the 'Acceptable Use Policy' before using any Federation ICT resources;
- All parents are required to sign the home-school agreement prior to their children being granted internet access within school;
- All visitors and students are asked to read and sign the Acceptable Use Policy prior to being given internet access within the school;
- The Federation maintains a current record of all staff and pupils who have been granted access to the Federation's internet provision.

Support for Parents

- Parents attention is drawn to the Federation's e-Safety policy and safety advice in newsletters, the Federation website, Piota app and e-Safety information workshops;
- The Federation website and app is used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website also provides links to appropriate online-safety websites.

Radicalisation Procedures and Monitoring

In accordance with the PREVENT strategy, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the DSL). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils.



The Winterton Federation e-Safety Policy



Sexual Harassment

Sexual harassment is likely to: violate an individual's dignity, make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children's Services may be notified.

Our Federation follows and adheres to the national guidance - UKCCIS: *Sexting in schools and colleges: Responding to incidents and safeguarding young people: Child on Child Sexual Violence and Sexual Harassment*.

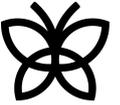
Further information can be found in the Dignity at Work policy.

Responses to Incident of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The Federation has incident reporting procedures in place and record incidents of an e-Safety nature on CPOMS. Staff and pupils are encouraged to use the following flow chart:



The Winterton Federation e-Safety Policy



Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the Federation's Behaviour and Discipline Policy. The Federation also reserves the right to report any illegal activities to the appropriate authorities



All Staff and Volunteer Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up 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 pupils/volunteers to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that all adults are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that Federation systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that all adults are protected from potential risk in their use of technology in their everyday work.

The Federation will try to ensure that adults have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect pupils/volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use Federation systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that The Winterton Federation will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the Federation digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Federation.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.



The Winterton Federation e-Safety Policy



I will be professional in my communications and actions when using The Winterton Federation ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Federation's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the Federation in accordance with the Federation's policies.
- I will only communicate with pupils and parents/carers using official Federation systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Federation has the responsibility to provide safe and secure access to technologies and ensure the smooth running of The Winterton Federation:

- When I use my mobile devices (laptops/tablets/mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the Federation about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the Federation ICT systems without seeking permission.
- I will not use USB devices whilst at the Federation.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant Federation policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. 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.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. I will not disable or cause any damage to Federation equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, where it has been agreed that I can do so, as outlined in the e-Safety policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Federation policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.



The Winterton Federation e-Safety Policy



When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of Federation digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Federation.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Federation digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the Federation) within these guidelines.

Name: _____

Position in school: _____

Signed: _____

Date: _____

e-Safety Policy Reviewed by: **The e-Safety Team Spring 2020**

Policy Accepted by Staff: **Spring 2020**

Policy accepted by governors: **Spring 2020**

Policy Review Date: **Spring 2022 or when changes are necessary to comply with Federation policy or national legislation.**