The Winterton Federation
Computing and e-safety Policy

Name and title of Author/s:	Shelly Goodall - Computing Lead Cheryl Baxter - Federation Business Manager
Name of responsible Committee/individual:	Recommended - Mrs Shelly Goodall
Implementation date:	Spring 2025
Review date:	Spring 2028
Targeted audience:	Parents/carers, staff, visitors and governing board
Related documents: All federation policies referred to are available on the federation website: https://thewintertonfederation.co.uk If English is not your first language, and you require assistance/translation, please contact the Junior school office.	PREVENT Strategy HM Government; MARS (Multi-Agency Resilience and Safeguarding board); 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; Keeping Children Safe in Education September 2024; The following federation policies: Safeguarding and Child Protection; Health and Safety; Whistleblowing; Behaviour; Anti-bullying; Mental Health and Well-being; Mobile Phone; Social Media; Bring Your Own Device; Data Protection; Discipline; Staff code of conduct.
Strategic alignment:	1.4 Objective: Continue to maintain a safe working and learning environment.

Contents

The Winterton Federation
Computing and e-safety Policy

At The Winterton Federation we endeavour to nurture unique individuals in a happy, safe, respectful and inclusive environment, where everyone is inspired to be the best they can be throughout their journey of life.

"Let us run with perseverance, the race that is set before us" (Hebrews 12:1)

We are all proud to be united in faith, vision and ambition.

Introduction
The 2014 national curriculum introduced a new subject, Computing, which replaces ICT. This represents continuity and change, challenge and opportunity. It gives schools the chance to review and enhance current approaches in order to provide an even more exciting and rigorous curriculum that addresses the challenges and opportunities offered by the technologically rich world in which we live. Computing Technology prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. We recognise that it is an important tool in both the society we live in and in the process of teaching and learning.

Computing is concerned with how computers and computer systems work, and how they are designed and programmed. Pupils studying computing gain an understanding of computational systems of all kinds, whether or not they include computers. Computational thinking provides insights into many areas of the curriculum, and influences work at the cutting edge of a wide range of disciplines.

The Acceptable Use Agreement (Appendix A) and the federation Safeguarding and Child Protection Policy should also be read in conjunction with this policy.

The Nature of Computing
The new National Curriculum presents the subject as one lens through which pupils can understand the world. There is a focus on computational thinking and creativity, as well as opportunities for creative work in programming and digital media.

The introduction makes clear the three aspects of the computing curriculum: computer science (CS), information technology (IT) and digital literacy (DL).

The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate - able to use, and express themselves and develop their ideas through, information and communication technology - at a standard suitable for the future workplace and as active participants in a digital world. Our vision is for all teachers and learners in our federation to become confident users of IT so that they can develop the skills, knowledge and understanding which enable them to use appropriate resources effectively as powerful tools for teaching and learning.

Computing in School
The National Curriculum for Computing has four main aims to ensure that all pupils:

- Can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation;
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems;
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems;
- Are responsible, competent, confident and creative users of information and communication technology.

Glossary of Terms

- Abstraction - Only focussing on the details relevant to the task, in computing this maybe by using a database to handle data.
- Logic - The non-arithmetic operations performed by a computer, such as sorting, comparing, and matching, that involve yes-no decisions. This might be completed using programs, such as Excel.

- Algorithms - The step-by-step procedure for a machine to complete a task, for example the instructions put into a bee-bot to guide it through a maze.
- Data Representation - The way in which information is presented. In its simplest form this could be representing a data set as a graph. However, it is also using the appropriate software for the task.

At The Winterton Federation we use Computing and Technology as a tool for learning, embedding the skills the children need to learn and experience into their everyday curriculum and exploration of our school themes and topics. The children learn to use and apply their skills into a real context, for example researching on the internet and attaching their own photography to their work. We aim to equip children to think creatively and use computing as a tool, to change, explore and develop their own knowledge. The children are also taught about the importance of technology safety and how to use it respectfully and responsibly. Also, they are taught what to do if they are concerned or worried about online content, safety or privacy.

Entitlement

The new National Curriculum states that pupils should be taught to:

	Key Stage 1	Key Stage 2
Computer Science	Understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous Instructions. Create and debug simple programs Use logical reasoning to predict the behaviour of simple programs.	Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts. Use sequence, selection, and repetition in programs; work with variables and various forms of input and output. Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs. Understand computer networks including the internet; how they can provide multiple services, such as the World Wide Web. Appreciate how [search] results are selected and ranked.
Information Technology	Use technology purposefully to create, organise, store, manipulate and retrieve digital content.	Use search technologies effectively. Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.
Digital Literacy	Recognise common uses of information technology beyond school. Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.	Understand the opportunities [networks] offer for communication and collaboration. Be discerning in evaluating digital content. Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Objectives

In order to fulfil the above aims it is necessary for us to ensure:

- A continuity of experience throughout the federation both within and among year groups;
- The systematic progression through key stage 2;
- That all children have access to a range of IT resources;
- That IT experiences are focussed to enhance learning;
- That cross curricular links are exploited where appropriate;
- That children's experiences are monitored and evaluated;
- That resources are used to their full extent;

- That resources and equipment are kept up to date as much as possible;
- That staff skills and knowledge are kept up to date.

Curriculum Development & Organisation
During a term, a class will work on completing one or two units of work based on the National Curriculum objectives for their year group. The National Curriculum, along with the Purple Mash scheme, is used to form the medium-term plans for Computing. Adaptations are made to ensure the plan is progressive in developing pupil capability. As well as a computer suite at WJS, there is a range of technology resources to enable the curriculum to be taught effectively. Resources are reviewed, replaced and updated when necessary. These devices encourage research, and allow for the creative use of ICT in subjects. Interactive touch screens are located in all of the classrooms.

Teaching & Learning
At TWF, computing is taught both as a discrete subject and in a cross-curricular way when the opportunity presents itself. A cross-curricular approach to planning is used throughout the curriculum and links into the termly themes (where possible) to make learning engaging and to give real life contexts for learning. Pupils are provided with opportunities to apply computing skills in other subjects.

The resources are distributed around the federation and are used to help pupils access the Computing curriculum, along with a range of other resources.

The Computing subject leader and the Executive Headteacher continually monitor the resources required to deliver the Computing element of the new National Curriculum. Planning is differentiated to meet the range of needs in any class including those children who may need extra support, those who are developing in line with age related expectations and those working securely for children of their age.

A wide range of styles are employed to ensure all children are sufficiently challenged:

- Children may be required to work individually, in pairs or in small groups according to the nature or activity of the task;
- Different pace of working;
- Different groupings of children - groupings may be based on ability (same ability or mixed ability);
- Different levels of input and support;
- Different outcomes expected.

The Computing subject leader reviews plans and examples of children's work to ensure a range of teaching styles are employed to cater for all needs and promote the development of IT capability. E-Safety is a thread of most IT work, in or out of computing lessons.

Equal Opportunities
The National Curriculum states that, "Lessons should be planned to ensure that there are no barriers to every pupil achieving." It is our policy to ensure this by:

- Ensuring all children follow the scheme of work for Computing;
- Keeping a record of children's work;
- Providing curriculum materials and software which are in no way class, gender or racially prejudice or biased.

Assessment
Computing is assessed both formatively and summatively. Formative assessment occurs on a lesson by lesson basis based on the lesson objectives. These are conducted informally by the teacher and are used to inform future planning. Teachers and support staff at TWF constantly assess children's progress in all curriculum areas and use this to inform their teaching. By the end of both Key Stages, pupils are expected to know, apply and understand the vocabulary, matters, skills and processes outlined in the National Curriculum Computing programme of study.

Assessment of children's work in Computing is ongoing and tracked using the Federation Assessment System. Achievement is reported to parents during the academic year. Children's work is saved to their Purple Mash folder for reference throughout the year.

Inclusion
We recognise IT and Computing offers particular opportunities for pupils with special educational needs and disability, gifted and/or talented children and/or children with English as an additional language for example. IT can cater for the variety of learning styles which a class of children may possess.

Using IT can:

- Increase access to the curriculum;
- Raise levels of motivation and self-esteem;
- Improve the accuracy and presentation of work;
- Address individual needs;
- Support children in keeping themselves safe.

We aim to maximise the use and benefits of IT as one of many resources to enable all pupils to achieve their full potential. Opportunities are provided for children to apply their skills in a range of different contexts throughout all curriculum areas.

Roles and responsibilities
Senior Leadership
The overall responsibility for the use of IT rests with the senior management of a school. The Executive Headteacher, in consultation with staff:

- Determines the ways IT should support, enrich and extend the curriculum;
- Decides the provision and allocation of resources;
- Decides ways in which developments can be assessed, and records maintained;
- Ensures that IT is used in a way to achieve the aims and objectives of the school;
- Ensures that there is a Computing policy, and identifies a Computing Subject Leader as well as an e-Safety Officer;
- Ensures that e-Safety messages are kept current and regular.

Computing Subject Leader
There is a designated Computing Subject Leader to oversee the planning and delivery within the federation. The Computing Subject Leader is responsible for:

- Raising standards in Computing as a national curriculum subject;
- Facilitating the use of IT across the curriculum in collaboration with all subject leaders;
- Providing or organising training to keep staff skills and knowledge up to date;
- Advising colleagues about effective teaching strategies, managing equipment and purchasing resources;
- Monitoring the delivery of the curriculum and reporting to the Executive Headteacher on the current status of the subject;
- Advising on new, recognised e-Safety dangers.

Teachers
It remains the responsibility of the teacher to plan and teach appropriate Computing activities and assist the subject leader in the monitoring and recording of pupil's progress.

Monitoring
Monitoring Computing enables the subject leader to gain an overview of teaching and learning throughout the federation. This assists the federation in the self-evaluation process identifying areas of strength as well as those for development. In monitoring of the quality of Computing teaching and learning the subject leader will:

- Scrutinise plans to ensure full coverage of curriculum requirements;
- Analyse children's work;
- Observe Computing teaching and learning in the classroom;
- Hold discussions with teachers;
- Analyse assessment data;
- Provide staff training through staff meetings and INSET training days on issues that arise from monitoring.

Health and Safety
We operate all IT equipment in compliance with Health and Safety requirements. Children are made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers. Computer Rules are also on display in all classrooms for reference along with specific rules for the use of internet and e-mail.

Each computer system has individual security against access to the management system. The files and network system are backed up regularly. The virus checker is updated regularly. Teachers ensure that pupils are taught and reminded, of the rules associated with appropriate use of equipment. A technician visits the federation weekly and repairs any items which are thought to be faulty. The federation's touch screens are located in classrooms.

All teachers have a laptop and iPad to use in school and at home. Teaching and learning staff are instructed to use One Drive for any information that includes personal details of pupils. The federation does not allow the use of encrypted memory sticks.

Technology and Infrastructure
In line with KCSIE 2023 appropriate filtering and monitoring systems are in place and checked regularly for effectiveness. Internet filtering is a key service and the federation has adequate approved filtering, anti-virus, anti-spam ware and firewall solutions installed on the network. The federation therefore;

- Maintain connection to a filtered broadband;
- Have additional user-level filtering in place;
- Ensures network health through the use of appropriate anti-virus software and regular technical checks;
- Ensure technical staff and administrators are up-to-date with services and policies;
- Never allows pupils to access internet logs;
- Never allows pupils to use any device without adult supervision;
- Use individual network logins for staff.

Management Information Systems (MIS)
IT enables efficient and effective access to and storage of data for the federation's management team, teachers and administrative staff. E-Safety protocols are adhered to e.g. passwords and back up. The federation has defined roles and responsibilities to ensure data is maintained, secure and that appropriate access is properly managed with appropriate training provided. Whole school assessment in all subjects is also stored electronically using the federation Assessment system.

Policy and Procedures
Due to the international scale and nature of the information available via the Internet, it is not always possible to guarantee that unsuitable material will never appear. Awareness of the risks, having the appropriate systems in place and supervising children in their use of the Internet are important considerations in reducing risk. The federation therefore:

- Supervises pupil's use of the internet at all times, and exercise extra vigilance on occasions when they have more flexible access, either by physical staff presence or use of a filtering and electronic monitoring system;
- Uses an appropriate and approved filtering system which blocks harmful and inappropriate sites;
- Exercises extra vigilance during raw image searches;
- Informs children that Internet use is monitored;
- Informs all users that they must report any failure of the filtering systems to the system administrator;
- Requires children and staff to individually sign an acceptable use agreement form which is fully explained to them;
- Makes the 'rules of appropriate use' clear to all users, at an appropriate level, and what sanctions will result from misuse;
- Keeps a record of any bullying or inappropriate behaviour for evidence in line with the federation Behaviour/e-Safety Policy;
- Ensures the designated Child Protection and E Safety Officers have appropriate training in e-safety;
- Ensures parents/carers provide consent for their child to use the Internet, as well as other IT;
- Makes information on reporting offensive materials, abuse, bullying etc. available to children, parents, carers and staff;
- Immediately refers any material we suspect is illegal to the appropriate authorities.

Education and Training
Even with all safety procedures in place, children will still occasionally download inappropriate material. Children and staff need to know how to respond responsibly, how to become 'Internet Wise'; to STOP and THINK before you CLICK. TWF therefore:

- Fosters a 'No Blame' environment that encourages children to tell an adult immediately they encounter any material they feel uncomfortable with;
- Ensures children and staff know what to do if there is a cyber-bullying incident;
- Ensures all children know how to report abuse;
- Has an e-Safety education programme, which is part of the Computing and wider curriculum. Through this, children are taught a range of skills and behaviours relevant to their age and experience;
- Ensures, when copying materials form the web, children and staff, understand issues of plagiarism and copyright;

- Offers e-Safety advice and guidance for parents/carers.

The Winterton Federation Internet Safety Rules

These rules help us to stay safe on the internet and when using computers and other mobile technology.

- We ask permission before using the internet.
- We try to check the reliability of information.
- We only use websites or apps our teachers have chosen for us.
- We tell an adult if we see anything we are uncomfortable with - do not delete.
- We will not look at, move or delete other people's files without their permission.
- We only e-mail or message people our teachers have approved.
- We only send emails and messages that are polite and friendly.
- We never give out any personal information (including photographs) or passwords - including 'pop ups.'
- We never arrange to meet anyone we don't know.
- We do not open files or emails sent by anyone we don't know.
- We do not use internet chat rooms.
- I will not respond to or add people I do not know personally.
- I will not use mobile phones in school; I will give mine to my classroom adult to keep safe if I bring it to school.

e-Safety

e-Safety Co-ordinator - Sheliza Goodall
Computing Co-ordinator - 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;
- Mental Health and Well-being;
- Mobile phone Policy;
- Social Media Policy;
- Data Protection Policy;
- Bring Your Own Device 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 2023;
- 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 federation community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our federation 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;
- 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 (Appendix A) which every pupil signs and is displayed throughout each federation school;
- Each federation school models 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 (Appendix A), 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 Federation 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 (Appendix A) 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 federation 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 Wavenet. 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 (Appendix A) 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;
- 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, pupils and governors 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, staff or governors 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 may 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 federation 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.

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 federation 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 with their classroom adult.

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;
- All staff complete and sign a Bring Your Own Device (BYOD) Request form.

CCTV
The Federation uses CCTV in some areas of the Junior school site as a security measure. Cameras are only used in appropriate areas and there is clear signage indicating where it is in operation. (Please see CCTV Policy).

General Data Protection (UK-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.

UK-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), Mr Tim Pinto, immediately, who may need to inform the Information Commissioner's Office (ICO).

Authorising Internet access
- All staff read and sign the 'Acceptable Use Policy (Appendix A)' 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 pupils are asked to read and sign the Acceptable Use Policy (Appendix A) 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, School Ping app and e-Safety information workshops;
- The federation website and app are 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 are 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.

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).

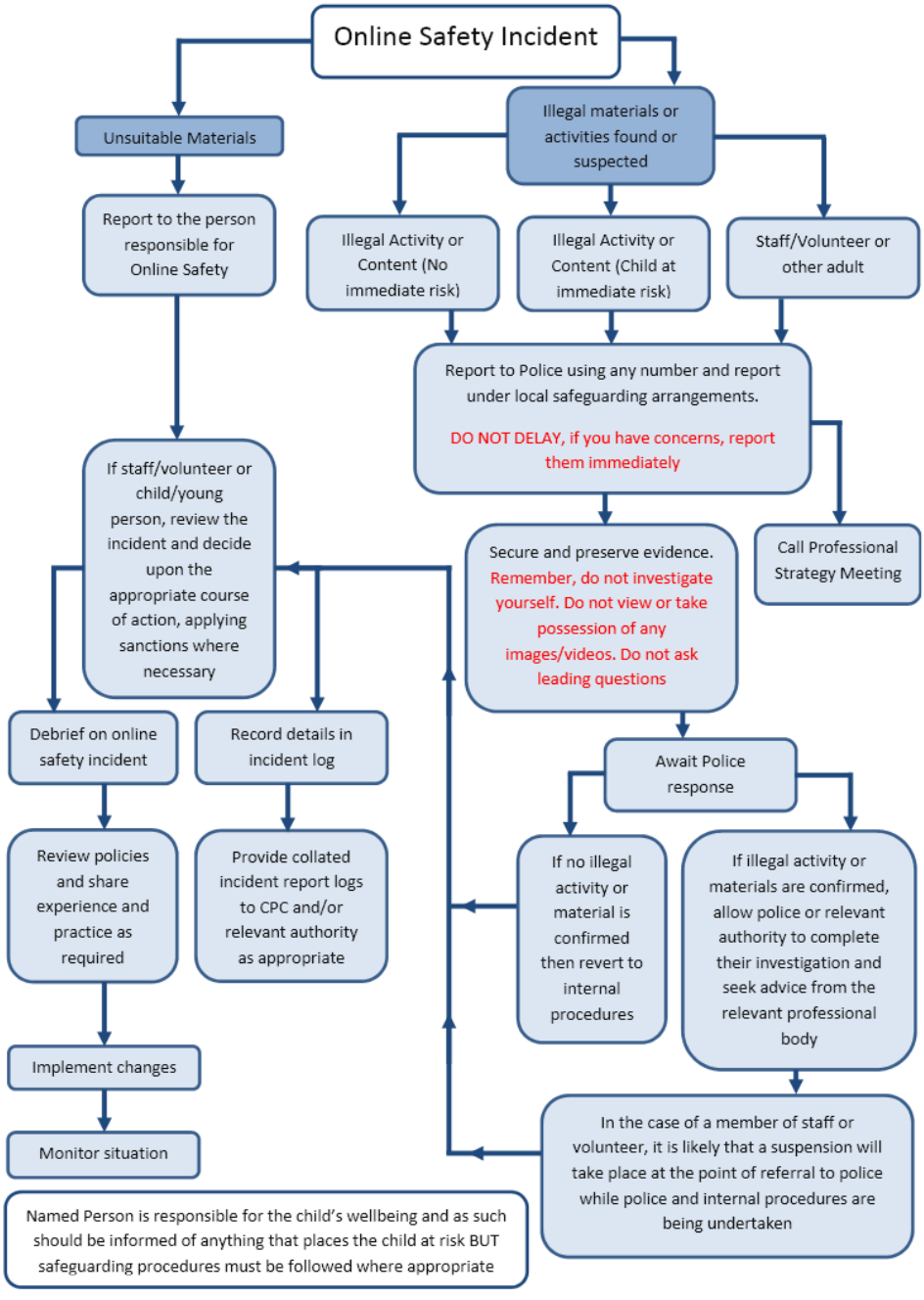
Any reports of online sexual harassment are taken seriously, and the police and Children's Services may be notified.

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 Mutual Respect 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:



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.

Review
The Executive Headteacher and staff will review this policy in accordance with the development priorities stated in the federation's Development Plan.

This policy will be reviewed every three years or in the light of changes to legal requirements.

Appendix A

All Staff and Volunteer Acceptable Use Agreement (AUA)

This agreement covers the use of digital technologies within The Winterton Federation: i.e. email, cloud platforms and network resources, learning platforms, software, artificial intelligence, digital equipment and systems. In addition, it also includes the use of personal devices to access federation information.

To protect users, the federation complies with the following legislation:

- Data Protection Act 2018 and General Data Protection Regulation (UK-GDPR);
- Privacy and Electronic Communications Regulations;
- Copyright, Designs and Patent Act 1988;
- Computer Misuse Act 1990;
- Counter-Terrorism and Security Act 2015 (encompassing the "Prevent Duty");
- The Regulation of Investigatory Powers Act (RIPA) 2000;
- Waste Electrical and Electronic Equipment Regulations 2006;
- The Environmental Protection Act 1990;
- The Waste Management Regulations 2006;
- The Department for Education Digital and Technology Standards for Schools and Colleges;
- Keeping Children Safe in Education (KCSIE).

General

- I will use the federation's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher and Governing board;
- If I am allowed access to the school's 'Wi-Fi', I will ensure that I follow the federation guidelines in accessing personal apps/sites;
- I will not allow unauthorised individuals to access emails, internet, network or other federation/ external systems;
- I will ensure that all sensitive or confidential documents and data are saved, accessed and deleted in accordance with the federation's data security and confidentiality protocols;
- I will not engage in any online activity that may compromise my professional responsibilities.

Email

- I will only use approved, secure email systems for federation business. I will not use personal email addresses for federation communication;
- I will only use approved federation email or Managed Learning Environment (MLE) or specified apps for communication with parents/carers, if necessary, e.g. trips or remote learning;

- I will ensure that I do not click on any random links via unsolicited emails that are sent to my federation email address;
- I will follow the federation's wellbeing procedures and, do not expect staff to respond to emails outside of their working hours.

Internet Access/Software

- I will follow procedures in relation to using school based mobile technologies;
- I will not browse, download or send material that could be considered offensive to colleagues;
- I will report any incidents relating to the bypassing of the federation school's filtering system;
- I will report any accidental access to, or receipt of inappropriate materials or filtering breach to the senior leadership team;
- I will not download any software or resources from the internet that can compromise the network or are software that the federation does not have a licence for.

Passwords

- I will not reveal my passwords to anyone except restricted authorised staff as and when the need arises;
- I will ensure that all passwords created are complex and include upper-case, lower-case letters, numbers and symbols;
- I will not write down passwords, but look at alternatives, such as password managers. I will only use password managers authorised by the federation.

Digital Devices

- I will not connect a computer, laptop, tablet or other device (including USB flash drive) to the network/internet that does not have an up-to-date anti-virus software;
    - External media must not be used in school unless verified as safe by the ICT team;
    - Anti-virus and firewall must not be disabled;
    - Encryption must not be bypassed.
- I will not bring in from home any other device, e.g. laptop, tablet, digital camera, unless I have been given authorisation by the Executive Headteacher;
- I will not allow children to access my federation laptop;
- I will not use my smartphone for taking images of pupils;
- I will ensure that my smartphone is stored away during lesson time in the classroom/locker;
- If I use a smart watch, I will ensure that it is on silent during lesson time;
- If I access school-based data on a personal device, e.g. smartphone, I will ensure that:
    - I enforce two factor authentications;
    - I will not use any 'jailbroken' phone;

- I will enforce factory reset if selling the device;
- I will alert the federation as soon as possible if I lose the device during term time and holidays.

Social Media/Messaging Services

- I will ensure that any private social networking sites/blogs that I create or actively contribute to are not confused with my professional role. Any use of these sites will not conflict with my professional role in the federation. I will ensure that my security settings are set to high;
- If the federation permits the use of messaging apps, such as WhatsApp, I will ensure that I adhere to rules, such as not using names of children;
- I will not run personal chat/network programs in the background whilst in either federation school;
- I understand that the following are all forms of social media:
  - Facebook;
  - Snapchat;
  - Instagram;
  - You Tube;
  - X (formerly Twitter);
  - Tik Tok;
  - WhatsApp.

Remote Learning

- I will ensure that any confidential data that I wish to transport electronically from one place to another is stored on SharePoint and two factor authentication is enforced. I will follow federation data security protocols when using such data in any location;
- I will follow the federation's procedures in any remote learning activity or meeting.

Data Protection

- I understand that data protection policy requires that information seen by me with regard to staff or pupils, held within the federation's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority;
- I will embed the federation's e-safety curriculum in to my teaching;
- I understand that all internet and network usage is logged and this information could be made available to the senior leadership team or governors on request;
- I understand that any information that is included in e-mails and cloud-based systems, e.g. CPOMS, could be included as part of a subject access request.

Artificial Intelligence

- I will ensure that I follow any procedures and policies about the use of Artificial Intelligence;
- I will not input any personal data about individuals, e.g. children's names, into any AI tool;
- I will inform any relevant member of staff of the use of AI tools in observations and performance management.

Cyber Security

- I will follow the federation's advice on ensuring that I practice strong cyber hygiene routines when using technology in school;
- I am aware of the procedures of dealing with a cyberattack and understand who to report this to.

Whistleblowing

- I understand that I am protected under the federation's Whistleblowing Policy, if I disclose a data security breach which has not been reported by another member of staff;
- I understand that failure to comply with this agreement may lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the federation's most recent data protection and online safety policies.

I agree to abide by all the points above.

I wish to have a federation e-mail account; be connected to the internet and be able to use the federation's ICT resources and systems.

I use a personal device to access school-based information YES/NO

Make/Model of device: _____

Full name: _____

Date: _____

Signature: _____

Authorised Signature (Executive Headteacher/Deputy Headteacher)

I approve this user in line with statements included in the AUP.

Full name: _____

Date: _____

Signature: _____