Hope Kindness Forgiveness Aspiration Love Courage Trust Respect Friendship

Drake Primary School and Little Pirates Child Care

We unlock opportunity and inspire everyone.

ONLINE SAFETY POLICY

Formally adopted by the Governing Board of:-	**Drake Primary School & Little Pirates Child Care**
Chair of Governors:-	**Carly Brien**
Created on:-	**July 2022**

We aim to provide:

- a school where learning is visible and children are safeguarded and nurtured
- a rigorous assessment system to ensure no pupil falls behind
- a diverse learning community where pupils, families and staff collaborate to refine practice and develop positive and rewarding relationships
- a workplace where staff contribute to professional learning communities; locally, nationally and globally.

So our mission is to:

- inspire the poets, geneticists and astronauts of the future
- ensure children are happy and healthy through our values and play
- develop a culture where reading for pleasure is for everyone
- make the arts a central component for children's lifelong learning
- build a curriculum of joy and curiosity

Headteacher: Mrs Louise Rosen

Drake Primary School and Little Pirates Child Care, Fairfields, Thetford, Norfolk, IP24 1JW Tel: (01842) 762055

office@drake.norfolk.sch.uk www.drake.norfolk.sch.uk

Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for Anti-bullying, Safeguarding and Child Protection, Social Media Use policy and the School's Code of Conduct.

The Headteacher, as the Designated Safeguarding Lead (DSL), alongside the Computing Lead, has an overview of online safety at Drake Primary School.

Our Online 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.

Documents on file (Appendices)

- Parent/Carer ICT Code of Conduct (Online Safety)
- Parental consent form 2022
- Removal of technology forms
- Guidance for taking photographs in school
- NCC Recommended online safety checklist
- E-Security Checklist
- Legal Frameworks surrounding online safety
- Non-statutory guidance surrounding online safety
- Online Safety Education programme at Drake Primary School

1. Introduction and Overview

Review and Monitoring

Our Online Safety Policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school.

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Drake Primary School and Little Pirates with respect to the use of technologies.
- safeguard and protect the children and staff.
- assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- have clear structures to deal with online abuse such as online bullying, in line with the school's behaviour/anti-bullying policy and Safeguarding policy.
- ensure that all school community members are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

Rationale

- The risks to pupils online could include: exposure to inappropriate content, promotion of harmful behaviours, hate content, inaccurate or illegal material, grooming and sexual exploitation, exposure to radicalisation, online bullying, awareness of a digital footprint, identity theft, breach of copyright, invasion of privacy and sharing of private content.

Scope

- This policy applies to all members of the Drake and Little Pirates community (including staff, students/pupils, volunteers, parents/carers, visitors, and community users) who have access to and are users of school technologies, both in and out of Drake and Little Pirates.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and available to all members of the school community.
- The policy is part of the school induction pack for new staff where appropriate.
- All staff or visitors must read and sign the Staff Code of Conduct before using any school technology resource.
- All pupils must create and agree upon a class online safety agreement at the beginning of each school year.
- Regular updates and training on online safety for all staff, including any revisions to the policy.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).
- Staff are given information about infringements in use and possible sanctions, including disciplinary. (Staff Code of Conduct).
- Pupils have their own code of conduct which covers online safety.
- Designated Safeguarding Lead (DSL) acts as the first point of contact for any safeguarding incident whether involving technologies or not.
- Any concern about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of computing, RSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience drawn from the UKCIS framework “Education for a Connected World” (2020). Project Evolve and National Online Safety (NOS) are used to provide staff with high-quality resources and pertinent CPD.
- will remind students about their responsibilities through the Online Safety Education programme and reference to the pupil created Online Safety Agreement.

- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology. Eg keeping passwords secure, logging off, filtering of content etc.
- teaches pupils to evaluate internet content for authenticity and to be critical of its contents.
- demonstrates to pupils how to publish and present themselves appropriately to a wider audience.
- teaches pupils how to report unpleasant or inappropriate internet content.

Staff and governor training

This school:

- makes regular up-to-date training available to staff on online safety issues and the school's Online Safety Education program.
- provides, as part of the induction process, all staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Code of Conduct.

Parent/Carer awareness and training

This school:

- provides information/advice for parents/carers for online safety on the school website.
- utilises the resources of National Online Safety (NOS) to ensure support is relevant and up to date.
- provides parent-specific training via NOS.

3. Communication of the policy

Introducing the Online Safety policy to pupils

- Appropriate elements of the Online Safety Policy will be shared with pupils through our online safety curriculum work.
- Our school online 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 online safety issues and how best to deal with them will be provided for pupils.

Staff and the Online Safety policy

- All staff will have access to the school's online safety policy and its importance explained.
- Regular updates and training on online safety shall be provided for all staff, including any revisions to the policy.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school's online safety policy in newsletters, the school brochure and on the school website and other online content.
- Parents and carers will from time to time be provided with additional information on online safety.

All staff, pupils, volunteers and parents/carers will be informed of the online safety concerns procedure through this policy.

4. Incident management

In this school:

- there is strict monitoring and application of the online safety policy, including the Code of Conduct as it relates to ICT and a differentiated and appropriate range of sanctions.
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school.
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- concerns of a child protection nature must be referred to a Designated Safeguarding Lead (DSL), following the School's usual safeguarding procedures; unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors.
- we will immediately refer any suspected illegal content or contact to the appropriate authorities – e.g. the Police, Local Authority. Safeguarding Team.
- any concerns about staff misuse must be referred to the Headteacher, in line with the school's whistleblowing policy.

5. Managing IT and Communication Systems

Managing internet access and filtering

- The school's internet access is provided by **ICT Solutions** and includes filtering appropriate to the age of pupils, in accordance with DfE guidelines. The school will work in partnership with **ICT Solutions** to ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable and updated as necessary.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and interlinked online content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor **ICT Solutions** can accept liability for the material accessed or any consequences of internet access.
- Virus protection will be updated regularly.
- If staff or pupils come across unsuitable online materials, the source/website must be reported to a DSL or Deputy DSL.

E-mail

This school:

- provides staff with an email account for their professional use, *e.g. nsix.org.uk* and makes clear personal email should be through a separate account.
- will also use anonymous e-mail addresses, for example, head@, office@

- will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- will ensure that email accounts are maintained and up to date.

Pupils' email

- We use school-provisioned pupil email accounts that can be audited and pupils will be reminded of this through the teaching of our online safety curriculum
- Pupils are taught about online safety and appropriate use of email both in school and at home.
- Pupils can use their email account to sign up to curriculum-relevant resources online.

Staff email

- Staff will use Local Authority (LA) or school-provisioned e-mail systems for professional purposes.
- Access in school to external personal email accounts may be blocked.
- We use county-level staff email accounts that can be audited by the Headteacher
- Staff are instructed never to use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data/file must be protected with security encryption.

Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will not currently have access to any online technology in school.

Google Classroom

- Staff are instructed to not use Google Classroom before 8:00 or after 16:00.
- Google Classroom is not the appropriate channel for parents to contact staff directly - this must come through the office/PSA.
- Staff answering work-related children's questions is permitted within the hours mentioned above.

Social networking Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

Pupils

- Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety education programme.
- Pupils are required to create and follow an appropriate pupil online safety agreement.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our additional communications materials when required.

6. Digital Content

Published content and the school website

- The school website will comply with the statutory DfE requirements.
- The contact details on the school website and other public sites should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Senior Leadership Team (SLT) will take overall editorial responsibility and ensure that the school's website and other related public content is accurate and appropriate.
- The school will seek to ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.
- Photographs of pupils published on the website do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Publishing photographs, images and work

- Written permission from parents or carers will be obtained before photographs or videos of pupils are published.
- Photographs that include pupils will be selected carefully. The school will look at using group photographs rather than full-face photos of individual children where appropriate.
- Pupils' full names or personal information will not be used on the school website or other public sites.
- Parents and carers should be clearly informed of the school policy on publishing images, both on school and independent electronic stores.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and ensured that they follow all relevant Safeguarding and Data Protection regulations before use in school is allowed.
- The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

7. Data Security and equipment

- Management information system access, storage and data transfer will comply with the UK Data Protection Act (2018) which covers the General Data Protection Regulation (GDPR).
- Permission needs to be sought from the Headteacher for school devices to be taken off the school premises. No encryption-level data will be stored on non-school-based external devices. The school will provide encrypted storage devices for sensitive data.
- Permission needs to be sought from the Headteacher for home devices to be used in school.

APPENDIX 1 - Parent/Carer ICT Code of Conduct

As the parent or carer of pupil(s) at Drake Primary School, I grant permission for my child to have access to use the internet, school email and other ICT facilities at school.

I know that my child is aware of the school's rules for responsible ICT use, outlined in their class' online safety agreement. I know that the latest copy is available on the school website and that further advice about safe use of the Internet can also be found there.

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,
safe access to email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, emails and the websites they visit. I also know that the school may contact me if there are concerns about my child's online safety or online 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 online safety.

Parent/carer signature: …….
Date: ……

APPENDIX 2 – Parental consent form 2022

Full name of Pupil
Year Group
Name of parent completing the form
Date

	Yes	No
At Drake pupils have regular opportunities to perform. Previously we have been involved in the live streaming of events at the O2 and the Royal Albert Hall. Images/videos may be used by external sources eg. local newspapers and digital press, I consent to images and videos being used in this way		
At Drake pupil images/videos may be taken and used by our school for display throughout the school building, on the school website and for brochures/prospectus. I consent to images and videos being used in this way		
I consent to images/videos being used on the school Twitter page		
I consent to share my child (s) data with a school-appointed external photography company to take individual, family and class photos		
I consent to local outings		
I confirm that I have read the school "Working Together Agreement" and Mission, Vision and Aims and agree to support our child in achieving this.		
I confirm that I have read the Forest School letter and information (found on the website) and discussed the content with my child		

Refreshing your consent

This form is valid for the period of time that your child remains at Drake Primary School. Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. a social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for
- Changes to the schools internal systems, such as MIS (Management Information System)

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the school office. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent

Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect any images or videos that have been shared prior to withdrawal.

If you would like to withdraw your consent, you must submit your request in writing to the school office.

APPENDIX 3 – Removal of technology agreement

Removal of Technology Agreement
Drake Primary School and Little Pirates

Details of machine(s) to be removed: -

Item 1 and make_____

Serial number _____

Item 2 and make_____

Serial number _____

I understand that by removing the piece(s) of technology from school property I am agreeing to the following conditions: -

1. The machine(s) will not be used for private purposes.
2. Passwords for the machine(s) will be kept secure and the machine(s) closed down when not in use.

3. The machine(s) will not be left unattended in a car unless doors, windows and other means of access are secured, locked and keys removed to a place of safety. The machine(s) must be placed in the boot or otherwise out of sight.
4. When stored at home, the machine(s) will not be visible from the outside of the building and the building will be locked securely when vacated.

Name _____

Signed _____

Date _____

APPENDIX 4 Guidance for Taking Photographs in School

Information Commissioner's Office Version: 4.1

Introduction

The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers to fully understand their obligations and promote good practice.

This guidance is aimed at Local Education Authorities and those working within schools, colleges and universities. It gives advice on taking photographs in educational institutions and whether doing so must comply with the DPA.

Recommended good practice

The DPA is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the DPA should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure.

Where the DPA does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official school use may be covered by the DPA and pupils and students should be advised why they are being taken.

- Photos taken purely for personal use are exempt from the DPA.

Examples

Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the DPA does not apply.
- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the DPA does not apply.

Official school use:

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the DPA will apply.
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the DPA as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Media use:

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the DPA.

More information

Additional guidance is available on our guidance pages if you need further information on other parts of the DPA.

This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.

APPENDIX 5 NCC Suggested Online Safety Checklist

This checklist can be used to carry out a very simple audit of the online safety provision in your school.

The responsible member of the Senior Leadership Team is: **Louise Rosen**	
The responsible member of the Governing Body is: **Carly Brien**	
Has the school got an online safety Policy that allies with Norfolk guidance?	**Yes**
When was the policy updated/reviewed?	
The school online safety policy was agreed by governors on:	
How is the policy made available for staff?: **School website**	
How is the policy made available for parents/carers?: **School website**	
Is a clear, progressive online safety education programme in place for all pupils?	**Yes**
Are all pupils aware of the School's ICT Code of Conduct?	**Yes**
Are online safety rules displayed in all rooms where technologies are used and expressed in a form that is accessible to all pupils?	**Yes**
Has up-to-date online safety training been provided within the last year for staff?	**Yes- Staff have been offered CPD to complete and those unable to attend will receive training within the Autumn Term**

Is there a clear procedure for a response to an incident of concern?	**Yes**
Do all staff receive and sign a Code of Conduct on appointment which includes the ICT Code of Conduct?	**Yes**
Do parents/carers sign and return an agreement that their child will comply with the School ICT Code of Conduct/Acceptable Use Policy?	**Yes**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Yes**
Is Internet access provided by an Internet service provider which complies with DfE/NEN requirements?	**Yes**
Have online safety materials from CEOP been obtained?	**Yes**
Is personal data collected, stored and used according to the principles of the Data Protection Act, following guidance provided by the ICO?	**Yes**
Where appropriate, have teaching and/or technical members of staff attended training on the school's filtering system?	**Yes**

Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Yes**

APPENDIX 6 E-Security Checklist

The Education Network (NEN) has produced a school e-security checklist, setting out 20 e-security controls that, if implemented effectively, will help to ensure that school networks are kept secure and protected from internal and external threats.
The advice presented here is adapted from the Council on Cyber Security's Critical Security Controls document. The description of each control is accompanied by two sets of questions: one for school network managers and support staff, and one for head teachers and senior leadership teams. The former are concerned with operational matters, while the latter focus on policy, strategy and budgetary considerations.

An accompanying document, 10 steps to protect your school's network – a guide for school leaders, provides a one-page overview of these controls for school senior leadership teams.

Through answering the following questions, our school is able to demonstrate how e-security is addressed.

Critical Security Control Questions for School	Questions for School Head Teachers, Senior Leaders and Governors
1. Inventory of Authorized and Unauthorized Devices: Actively manage (inventory, track, and correct) **all hardware devices** on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	Does your school's Staff Code of Conduct include provisions/instructions to ensure only authorised devices are connected to the school's network? This is made clear in our ICT code of Conduct.
2. Inventory of Authorized and Unauthorized Software: Actively manage (inventory, track, and correct) **all software on the network** so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	Does your school's Staff Code of Conduct include provisions/instructions to ensure only authorised devices are connected to the school's network? This is in our ICT Code of Conduct.

3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Does your school's Staff Code of Conduct include clear provisions/instructions warning users about tampering with secure configurations, with clear sanctions for any infraction? This is made clear in our ICT Code of Conduct. Do you have visibility of likely costs to upgrade and refresh hardware and software as necessary, and when these costs are likely to be incurred (for example, antivirus software subscriptions, firewall support and maintenance services, dates for when hardware/software will go "end of life" and need to be replaced)? This is taken into account through our Asset Register and looking at needs of the setting.

4. Continuous Vulnerability Assessment and Remediation: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	Do you have processes in place for regular review of e-security functions and your IT acceptable use policies to address new and emerging threats? How do you ensure staff and pupils receive appropriate e-security advice and training? This is done through the following: • ICT solutions • Netsweeper • ICT Technician • The school curriculum and Online Safety policy.
5. Malware Defences: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.	How do you ensure that your Staff Code of Conduct are up to date to minimise risks in this area? The setting follows county advice. What sanctions are applied for malicious use of school IT services and systems? This would be under the school's disciplinary and safeguarding procedures.
6. Application Software Security: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses	Do you have visibility of when significant upgrade and renewal of software will be required, both in terms of likely cost and ensuring service continuity? Planning in budget and advice from ICT technician. How do you ensure staff and pupils are trained in the use of new software? As needed

7. Wireless Access Control: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	What is the school's policy on wireless access – do you allow guest access, or access from staff- or pupil owned devices? No Does your Staff Code of Conduct appropriately encompass access from staff- or pupil-owned devices if this is allowed? If children bring in their own devices, they must be handed to staff or placed in a locker at the beginning of the day. Do your staff and pupils understand their obligations and responsibilities in relation to using their own devices in school, if they are allowed to do so? For staff, this information can be found in the Staff Code of Conduct. Children know that devices cannot be used in school.
8. Data Recovery Capability: The processes and tools used to back up critical information properly with a proven methodology for timely recovery.	Does your school have an overarching disaster recovery/business continuity plan? Yes If so, does this encompass restoration of IT facilities and critical school data appropriately? Yes
9. Security Skills Assessment and Appropriate Training to Fill Gaps: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	Does your school's overarching staff training and development planning include provisions to ensure that technical support staff can keep up to date with e-security risks and best practices and that all teaching and administrative personnel understand their own security obligations and responsibilities? The setting has an ICT technician for 1 day a week from ICT solutions who is kept up to date on this. Teaching and Admin staff are aware of own e-security, obligations and responsibilities, this is mainly through the Code of Conduct.

10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Do you have visibility/awareness of when major changes and/or upgrades will need to be carried out, in terms of both likely cost/budgeting and maintaining service continuity? This is done through ICT solutions and employing their ICT technician.

11. Limitation and Control of Network Ports, Protocols, and Services: Manage (track/control/correct) the on-going operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	Do you have visibility of when major changes are likely to be necessary? ICT Solutions and IT technician Do you have effective processes for communicating changes, for example in relation to changing security settings to allow access to a new service or facility – are appropriate risk assessment and management processes in place and adhered to? Yes
12. Controlled Use of Administrative Privileges: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	Do you have effective strategies in place to ensure the importance of administrator privileges are understood and respected? Yes Does your ICT Code of Conduct/acceptable use policy (AUP) require strong, complex passwords and regular password changes? This is in our Code of Conduct. Changed at least once a year.
13.Boundary Defence: Detect/prevent/correct the flow of information transferring networks of different trust level with a focus on security damaging data.	Do you employ any independent third party testing of your boundary defences to maintain their effectiveness in the light of dynamic and emerging threats? ICT Solutions

14.Maintenance, Monitoring, and Analysis of Audit Logs: Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.	How do you ensure that sufficient time is allocated to reviewing and acting upon the outputs from monitoring and logging activities? ICT Technician Where do responsibilities for reviewing outputs from monitoring and logging reside? SLT and ICT technician What are your data retention policies, and where are they described? Data Protection Policy
15. Controlled Access Based on the Need to Know: The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	Does your ICT Code of Conduct/online safety agreements differentiate between the obligations and responsibilities of different groups of users (teaching staff, administrative/managerial staff, pupils, governors)? Yes How do you communicate with and keep different user groups up to date with their obligations and responsibilities? Code of Conduct written for different groups of users.

16. Account Monitoring and Control: Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	Do you undertake any monitoring of user accounts for unusual usage? The setting has signed up for this from ICT Solutions. We should be informed of any issues by them. How do you communicate with, educate and inform different user groups of their obligations and responsibilities? Through Code of Conduct, Online Safety Policy (2022), CPD and curriculum.
17. Data Protection: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information (exfiltration: the unauthorized release of data from within a computer system or network)	Are all staff and pupils aware of all their responsibilities and obligations in relation to sensitive and personal data, particularly in the light of schools' roles as data controllers under The Data Protection Act 1998? This is made aware to staff and pupils in Data Protection Policy available to read.
18. Incident Response and Management: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	How regularly are incident handling processes reviewed? Do you undertake any example incident scenarios to test and update incident handling processes and procedures? Systems are checked weekly by ICT technician. Systems also monitored by ICT Solutions
19. Secure Network Engineering: Make security an inherent attribute of the enterprise by specifying, designing, and building--in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.	How much and how often are time and resources allocated to reviewing and updating the school network as a whole? What processes and analysis are employed to determine which security functions are best provided 'in house' and which should be delivered using the expertise of third parties such as broadband service providers? The setting buys into ICT Solutions and follows their advice and guidance.
20. Penetration Tests and Red Team Exercises: Test the overall strength of an organization's defences (the technology, the processes, and the people) by simulating the objectives and actions of an attacker	How do you identify sources of advice and support that can scrutinise the security of you network and suggest an action plan for improvement? ICT Solutions

APPENDIX 7 - Online Safety Programme

Online safety is built into the culture of Drake and its class communities. Classes develop individual online safety agreements that specifically reflect the children and their online spaces.

Online safety provision at Drake follows the UK Council for Internet Safety's (UKCIS) "Education for a Connected World" (2020) framework. As such, each year group engages with the following strands:

- Self-Image & Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Wellbeing & Lifestyle
- Privacy & Security
- Copyright & Ownership

We use Project Evolve knowledge maps to regularly assess classes and identify areas with which the children need further support. This allows all of our online safety delivery to be bespoke, targeted and relevant.

Teachers plan responsive lessons using resources from both Project Evolve and NOS.

APPENDIX 8 - The Legal Framework Surrounding Online Safety

This section is designed to inform users of legal issues relevant to the use of electronic communications.

Voyeurism (Offences) Act 2019

The Voyeurism (Offences) Act 2019 creates 2 new offences criminalising someone who operates equipment or records an image under another person's clothing (without that person's consent or a reasonable belief in their consent) with the intention of viewing, or enabling another person to view, their genitals or buttocks (with or without underwear), where the purpose is to obtain sexual gratification or to cause humiliation, distress or alarm.

Data Protection Act 2018 (replacing the Data Protection Act 1998)

The Act implements GDPR standards across all general data processing and ensures that sensitive health, social care and education data can continue to be processed while making sure that confidentiality in health and safeguarding situations is maintained

In implementing the GDPR standards, the Act requires organisations that handle personal data to evaluate the risks of processing such data and implement appropriate measures to mitigate those risks. For many organisations such measures include effective cyber security controls.

Education and Inspections Act 2006, sections 90 and 91,

Provides statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. **Section 94** also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with E-safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from abuse based on their race, nationality or ethnic background.

Sexual Offences Act 2003

A new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and then intentionally meet them or travel with intent to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fa ll in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. Schools should already have a copy of “Children & Families: Safer from Sexual Crime”.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Relationships Education, Relationships and Sex Education (RSE) and Health Education 2021

This legislation sets out to ensure that children, through the curriculum, teaching and other means of learning, are aware of the distinction between real and online worlds and understand how they differ from each other. This legislation should also enable teachers to create a culture of awareness to emphasise to children that information online may be false or misleading and also the personas that others portray online have the potential to also be false and misleading. The positives of the online environment are also emphasised and children should be shown how to gain the most of their positive experiences online.

APPENDIX 9 – Non-statutory guidance surrounding Online Safety

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- DfE (2021) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- DfE (2017) 'Preventing and Tackling bullying'
- DfE (2014) 'Cyberbullying: Advice for headteachers and school staff'
- Harmful challenges and online hoaxes (2021)
- Ofsted (2021) Inspecting safeguarding in early years, settings and skills
- Ofsted (2013) 'Inspecting e-safety'
- Safer Recruitment Consortium (2022) 'Guidance for safer working practice for those working with children and young people in education settings'
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (2020)
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety 'Education for a Connected World' (2018)
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'