Wakefield Grammar School Foundation

Document Reference	**ICT Acceptable Use Policy**
Version Number	V2.0
Author/Lead **Job Title**	John Lister, Digital Services Technical Director
Checker Person Name **Quality Assurance**	Jenny Cocker, Director of Finance and Operations
Consultation	Designated Safeguarding Leads Compliance Manager / Data Protection Officer JNCC
Name of Approver/Committee **Date Ratified**	Gov. Board **19.06.2024**
Date of Next Review (2 yearly)	**June 2026**

VALIDITY – Policies should be accessed via Firefly to ensure the current version is being used.

CHANGE RECORD - REVIEW PERIOD (2 yearly)

Version	Date	Change details
V2.0	May 2024	Policy reviewed and re-written.

To be published on the following:

Staff shared	**X**	**Website**	**X**

WGSF ICT Acceptable Use Policy

1. Scope of this Policy

This policy applies to all members of the Foundation community, including staff, pupils, parents and visitors, who have access to and are users of the Foundation ICT systems. In this policy:

- “staff” includes teaching and support staff, governors, and volunteers;
- “parents” includes pupils' carers and guardians; and
- “visitors” includes anyone else who comes to the Foundation.

This policy covers both fixed and mobile internet devices provided by the Foundation (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto Foundation premises (personal laptops, tablets, smart phones, etc.).

Access to Foundation systems is not intended to confer any status of employment on any contractors.

1.1 Compliance with related Foundation policies

This policy is implemented to protect the interests and safety of the whole Foundation community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following Foundation and School policies:

- WGSF Safeguarding and Child Protection Policy
- WGSF Data Protection Policy
- WGSF Privacy Notices
- WGSF Staff Code of Conduct
- WGSF Educational Visits Policy
- Schools’ Behaviour Policies
- Schools’ PSHEE / RSE Policies

2. Online behaviour

As a member of the Foundation community you should follow these principles in all of your online activities:

- The Foundation cannot guarantee the confidentiality of content created, shared and exchanged via Foundation systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the Foundation community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).

- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the Foundation community, even if the content is not shared publicly, without going through official channels and obtaining permission.

- Do not create, publish, save, and/or share live stream training videos/presentation slides involving sensitive pupil data taken from WGSF systems such as SIMS or CPOMS.

- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Please consult the Online Safety Section of this document, in Annex 1, for more details.

3. Using the Foundation's ICT systems

Whenever you use the Foundation's ICT systems (including by connecting your own device to the network) you should follow these principles:

- Only access Foundation ICT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the Foundation's ICT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, Foundation ICT systems.
- Do not use the Foundation's ICT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the Foundation monitors use of the Foundation's ICT systems, and that the Foundation can view content accessed or sent via its systems.
- Files not related to Foundation activities should not be stored on Foundation Storage. Please be aware that files stored on Foundation Storage (Google Drive, One Drive, Sharepoint, Gmail and other systems) are subject to access from other members of the Foundation and delegated support providers for regulation, antivirus, antimalware, disciplinary, investigation or business continuity purposes.

4. Passwords

Passwords protect the Foundation’s network and computer system and are your responsibility. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else’s computer or to confidential information to which you do not have access rights.

All pupils and members of staff should:

- use a strong password (usually containing ten characters or more, and containing upper- and lower-case letters as well as numbers); They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords.
- not write passwords down; and
- not share passwords with other pupils or staff.

Modifications to Password length and complexity may be made to take account of the age of the pupils and other authentication mechanisms may be used which may also limit their access.

5. Multi Step Authentication

Staff must use multi factor authentication as directed by Digital Services. You should not let anyone else use your token.

6. Use of Property

Any property belonging to the Foundation should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to Digital Services.

7. Use of Foundation systems

The provision of Foundation network, email accounts, Wi-Fi and internet access is for official Foundation business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their Foundation ICT use and limit as far as possible any personal use of these accounts. Again, please be aware of the Foundation's right to monitor and access web history, network and email use.

Further information can be found in Annex 1 of this document.

8. Use of personal devices or accounts and working remotely

All official Foundation business of staff must be conducted on Foundation systems, and it is not permissible to use personal accounts for Foundation business. Any use of personal devices for Foundation purposes, and any removal of personal data or confidential information from Foundation systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick must be approved by the Director of Finance and Operations or the Data Protection Officer.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the Foundation's policies, including two-factor authentication, encryption etc.

Please consult Annex 1 of this document and the Foundation's Bring Your Own Device (BYOD) Policy for more information.

9. Monitoring and access

Staff, parents and pupils should be aware that Foundation email and internet usage (including through Foundation Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and Foundation network drives and email accounts and other services may be accessed by the Foundation where necessary for a lawful purpose – including business continuity, serious conduct or welfare concerns, extremism and the protection of others.

See Annex 1: Online Safety, for further details.

10. Tracking Devices and Technology

The Foundation is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Use of this technology in the context of Foundation activities is limited for safeguarding on trips with added risk such as those pupils on Duke of Edinburgh awards expeditions, but if parents do plan to

use it personally then they should be aware of potential third party privacy considerations and only use it for domestic / personal purposes in respect of their own child and/or their or their child's belongings.

11. Breach reporting

The law requires the Foundation to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the Foundation regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the Foundation's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected email or postl;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The Foundation must report certain types of personal data breaches (those which risk an impact to individuals) to the ICO within 72 hours. In addition, controllers must notify individuals affected if that risk is high. In any event, the Foundation must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they should contact the Data Protection Officer and Digital Services as soon as possible..

Data breaches will happen to all organisations, but the Foundation must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The Foundation's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but a failure to report a breach could result in significant exposure for the Foundation, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

12. Breaches of this policy

A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter (please refer to the WGSF Discipline and Conduct Policy and Procedure). In addition, a deliberate breach by any person may result in the Foundation restricting that person's access to Foundation ICT systems.

If you become aware of a breach of this policy, or you are concerned that a member of the Foundation community is being harassed or harmed online you should report it to the Designated Safeguarding Lead or Director of Finance and Operations. Reports will be treated in confidence wherever possible.

13. Acceptance of this policy

Users will be provided with access to a form when they join the Foundation and also periodically to reaffirm their acceptance of the policy.

Annex 1 : Online Safety.

1. Aims and Objectives

It is the duty of the Foundation to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies.

In the Foundation, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

In designing this policy, the Foundation has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the Foundation recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at Foundation. The improper use of technology by pupils, in or out of Foundation, will be dealt with under the Schools' Behaviour Policies and / or the Foundation's Safeguarding and Child Protection Policy as is appropriate in the circumstances.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the Foundation's Safeguarding and Child Protection Policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Foundation's Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Foundation's Safeguarding and Child Protection Policy. The Governing Body of the Foundation is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the, DSL and Senior Leadership Team are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the Foundation procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the Foundation.

3.2. The Executive and the Senior Leadership Team

The Executive Team is responsible for the safety of the members of the Foundation community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for safeguarding and child protection at each of the Foundation Schools. This includes a responsibility for online safety as well as the Foundation's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Senior Leadership Team and Digital Services staff to achieve this. As such, in line with the Foundation's Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with Digital Services to ensure that the Foundation's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that regular checks are properly made of the system.

The DSL will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures.

3.4. Digital Services

The Foundation's Digital Services staff have a key role in maintaining a safe technical infrastructure at the Foundation and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the Foundation's hardware system, its data and for training the Foundation's teaching and administrative staff in the use of IT. They may monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DSL or appointed representative.

3.5. Teaching and support staff

All staff are required to agree to this ICT Acceptable Use Policy before accessing the Foundation's systems. As with all issues of safety at this Foundation, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this ICT Acceptable Use Policy and enforce it in accordance with direction from the DSL and the Director of Finance and Operations as appropriate.

3.6. Pupils

Pupils are responsible for using the Foundation ICT systems in accordance with this Policy. Age appropriate rules for use are shared with pupils to give clear guidance where they would be unable to access this full policy and is conducted through the curriculum.

3.7. Parents and carers

The Foundation believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. The Foundation will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

In general:

The Foundation aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the Foundation's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the Foundation's filtering and monitoring systems apply to all users, all Foundation owned devices and any device connected to the Foundation's network. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Schools' Behaviour Policies, as appropriate.

Digital Services will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding governor or the DSL will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The Foundation's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as, but not limited to, other age inappropriate material or other content the Foundation deems so. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the DSL for their consideration.

The Foundation will monitor the activity of all users across all of the Foundation's devices or any device connected to the Foundation's internet server allowing individuals to be identified. In line with the Foundation's Data Protection Policy and Privacy Notices, Digital Services (and where appropriate, DSLs) will monitor the logs. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Foundation's Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the Digital Services Team if they believe that appropriate teaching materials are being blocked or which might generate unusual internet traffic activity.

Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to their teacher / DSL. Deliberate access to any inappropriate materials by a pupil will be dealt with under the School's Behaviour Policy. Pupils should be aware that all internet usage via the Foundation's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the Foundation's filtering system. If this causes problems for Foundation work / research purposes, pupils should contact their teacher for assistance.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The Foundation may require staff to conduct searches of their personal accounts or devices if they were used for Foundation business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

5. Education and training

5.1. Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the Foundation's expectations.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following this policy. All staff must sign and return the ICT Acceptable Use form to agree to this policy before use of technologies in Foundation.

All staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, or online courses, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about online safety as part of their safeguarding briefing on arrival at Foundation.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the Foundation community. When pupils use Foundation computers, staff should make sure children are fully aware of the agreement they are making to follow the Foundation's ICT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The Foundation provides opportunities to teach about online safety within a range of curriculum areas and IT / Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside the Foundation will also be carried out via presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see the School's Anti Bullying Policies, which describe the preventative measures and the procedures that will be followed when the Schools discover cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other Foundation staff for advice or help if they experience problems when using the internet and related technologies.

5.3. Parents

The Foundation seeks to work closely with parents and guardians in promoting a culture of online safety. The Foundation will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

6. Use of Foundation and personal devices

Staff

Foundation devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the Foundation device which is allocated to them for Foundation work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff at WGSF are permitted to bring in personal devices for their own use. Staff may use such devices in a way which doesn't detrimentally affect their Foundation work or that of others. Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recordings of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with the WGSF Safeguarding and Child Protection Policy, the WGSF Staff Code of Conduct and School Rules.

Pupils

Pupils are responsible for their conduct when using Foundation issued or their own devices. Any misuse of devices by pupils will be dealt with under the Schools' Behaviour Policies.

The Foundation recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with Learning Support to agree how the Foundation can appropriately support such use. Learning Support will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

7. Online Communications

Staff

Any digital communication between staff and pupils or parents must be professional in tone and content. Except for the work of the Foundation's Development Office who engage with Alumni, other members of staff are advised that they should continue to exercise caution when engaging with former students. The Foundation's advice is not to contact current or recent (alumni - less than 2 years since leaving) students directly. This would include contact on social media or online contact. Failure to properly consider any subsequent contact could harm both the reputation of the employee and the Foundation. Staff are advised to report to the DSL / Head if any contact is made by students directly to staff (this includes contact via social media).

The Foundation ensures that staff have access to their work email address when offsite, for use as necessary on Foundation business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and recent alumni. Under no circumstances may staff contact a pupil or parent / carer and recent alumni using a personal telephone number, email address, or other messaging system, nor should pupils, parents and recent alumni / their parents be added as social network 'friends' or similar. Please also refer to the WGSF Staff Code of Conduct.

Staff must immediately report to the DSL or Director of Finance and Operations the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to Digital Services (Staff should NOT forward the email. They should take a screenshot and report that to the helpdesk) .

Any online reputational issues encountered such as Trademark Violation, Impersonation, threats, targeted abuse and harassment and other allegations should be reported to the Data Protection Officer / DSL or Director of Finance and Operations. Further guidance released to support schools with online reputational concerns can be found here.

Pupils

All pupils are issued with their own personal Foundation network account for use on our network and related services. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work assignments / research / projects. Pupils should be aware that email communications through the Foundation network and Foundation email addresses are monitored.

The Foundation will ensure that there is appropriate and strong ICT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact their teacher for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to a member of staff who should then refer it to the DSL.

8. Use of social media

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with Foundation work or business from Foundation devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room/staff-only areas of the Foundation.

When accessed from staff members' own devices / off Foundation premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the Foundation in accordance with the Foundation's Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Wakefield Grammar School Foundation into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Foundation's Staff Code of Conduct or the Foundation's Safeguarding and Child Protection Policy.

Pupils

The Foundation expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The Foundation takes misuse of technology by pupils very seriously and incidents will be dealt with under the Schools' Behaviour Policies, Anti-Bullying Policies and the Foundation's Safeguarding and Child Protection Policy as appropriate.

Data protection

Please refer to the Foundation's Data Protection policy and the Foundation's Privacy Notices for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the Foundation.

Staff and pupils are expected to save all data relating to their work to their Foundation network account or to the Google Drive / Microsoft Onedrive Account or other Foundation systems as per this policy.

Staff devices should be encrypted if any data or passwords are stored on them. The Foundation expects all removable media (USB memory sticks, CDs, portable drives) taken outside the Foundation or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the Foundation.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the Foundation's ICT security and/or put at risk sensitive personal data (and other information) held by the Foundation. If in any doubt, do not open a suspicious email or attachment and notify the Digital Services Team.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Digital Services Team.

9. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites).

10. Artificial Intelligence

The Foundation is developing the use of Artificial Intelligence (AI) rules for staff and pupils. Use of such tools are subject to examining body regulations and other Foundation rules and policies.

In particular, personal or confidential information should not be entered into generative AI tools. This technology stores and learns from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff.

11. Misuse

The Foundation will not tolerate illegal activities or activities that are in breach of the Foundation's and Schools' policies. Where appropriate the Foundation will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The Foundation will impose a range of sanctions on any pupil or staff member who misuses technology to bully, harass or abuse another pupil in line with the Foundation's Safeguarding and Child Protection Policy and Schools' Behaviour policies.

12. Complaints

As with all issues of safety at the Foundation, if a member of staff, a pupil or a parent has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Please see the WGSF Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Foundation's Safeguarding and Child Protection policy and reported to the school's DSL.