Grace Academy Solihull

Digital Policy
(Incorporating Online Safety)

Policy Reference:	GA–P113
Status:	Operational
Applicable to:	Grace Academy Solihull
Authors:	M DAVIES-FRIEND
Checked By:	LGB
Valid From	March 2023
Review Date:	March 2024

Table of Contents

1. Introduction and aims

ICT is an integral part of the way our academy works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the academy.

However, the ICT resources and facilities our academy uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the academy community engage with each other online
- Support the academy's policy on data protection, online safety and safeguarding
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems
- Support the academy in teaching pupils safe and effective internet and ICT use

This policy covers all users of our academy's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour policy/staff code of conduct

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for academies

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the academy to use the ICT facilities, including governors, staff, pupils, parents, volunteers, contractors and visitors

"Personal use": any use or activity not directly related to the users' employment, study or purpose

"Authorised personnel": employees authorised by the academy to perform systems administration and/or monitoring of the ICT facilities

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

"Social Media Accounts": the academy currently defines this as Facebook, Twitter, Instagram and other platforms including, but not limited to, Tik Tok and Snapchat.

"BYOD": bring your own device – a device that is not provided by the academy for the purpose of teaching and learning.

4. Unacceptable use

The following is considered unacceptable use of the academy's ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the academy's ICT facilities includes:

- Using the academy's ICT facilities to breach intellectual property rights or copyright
- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, its pupils, or other members of the academy community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the academy
- Using websites or mechanisms to bypass the academy's filtering mechanisms

This is not an exhaustive list. The academy reserves the right to amend this list at any time. The principal will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of academy ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the principal's discretion.

Such requests should initially be discussed with the ICT Lead or Principal.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy's Student Behaviour Policy, Academy Charter and Staff Code of Conduct.

In some instances, this may be removal of permissions for using a device within the academy or removing permissions on the system.

Copies of the academy's Student Behaviour Policy, Academy Charter and Staff Code of Conduct can be found on the academy website.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to academy ICT facilities and materials

The academy's ICT Support team manages access to the academy's ICT facilities and materials for academy staff. That includes, but is not limited to:

Computers, tablets and other devices

Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the academy's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Support team.

Initial requests should be made through the ICT helpdesk support@tovelearning.org.uk

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (A special character is defined as any non-alphanumeric character that can be rendered on a standard English keyboard.)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring any alerts re: anti-virus and anti-spyware software expiring are passed to the ICT team
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 4.

Work devices should be used solely for work activities, except in cases in line with the agreed personal use guidelines detailed in section 5.2 Personal Use below.

If staff have any concerns over the security of their device, they must seek advice from The ICT Manager.

5.1.1 Use of phones and email

The academy provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the academy has provided.

Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff must not take images of students on their phones.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the ICT Support team immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the academy to conduct all work-related business.

Academy phones must not be used for personal matters.

The academy has the capacity to record in-coming and out-going phone conversations.

If a call is to be recorded, callers **must** be made aware that the conversation is being recorded and the reasons for doing so.

Explain when you record phone conversations and why. For instance:

"All calls to the academy office are recorded to aid administrators"

"Calls are recorded for use in staff training"

At present calls are not recorded, but the academy reserves the right to amend this providing the above comments are adhered to.

Interviews and discussions may be recorded to aid transcription, these are deleted once the transcript has been approved.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

Requests may include, but are not limited to, the following:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs assessments, etc.
- Discussing requests for term-time holidays

5.2 Personal use

Staff are permitted to occasionally use academy ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The ICT Lead or principal may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

Does not take place during contact time

Does not constitute 'unacceptable use', as defined in section 4

Takes place when no pupils are present

Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the academy's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the academy's ICT facilities for personal use may put personal communications within the scope of the academy's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the academy's Mobile phone use. See Appendix 5.

Staff should be aware that personal use of ICT (even when not using academy ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the academy's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times, including but not limited to taking account of the contents of this policy.

The academy has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1). Staff should apply equal care and consideration to other social media accounts, and should ensure that adequate privacy settings are in place.

5.3 Remote access

Staff are able to access the academy's ICT facilities and materials remotely.

Remote access to the academy system will be provided with the below conditions:

The remote access is provided through OpenVPN

Security arrangements include authentication using the school login and password

Protocols for remote access are the same as in school as the device is attached as it would be within the academy

Software is configured on the staff laptop and staff are provided with guidance on how this is done

Staff should ensure they follow the same etiquette and protocols when working remotely as when they are working within the academy building

Staff accessing the academy's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the academy's ICT facilities outside the academy and take such precautions as the ICT Support team may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The academy data protection policy can be found on the academy website.

5.4 Academy social media accounts

The academy has an official Facebook/Twitter and Instagram page, managed by a member of the academy leadership team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The academy also has other official twitter feeds, e.g. PE, managed by the HOD to provide details of events etc...

The academy has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of academy network and use of ICT facilities

The academy reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

Internet sites visited

Bandwidth usage

Email accounts

Telephone calls

User activity/access logs

Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The academy monitors ICT use in order to:

Obtain information related to academy business

Investigate compliance with academy policies, procedures and standards

Ensure effective academy and ICT operation

Conduct training or quality control exercises

Prevent or detect crime

Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

The Principal will have the opportunity to review the Grace Academy ICT system security annually.

If the case of absence from the academy, a staff member's web-based access may be frozen. Should there be any cause for concern the Principal may at their discretion instruct the Senior ICT Technician to freeze access for this member of staff instantly.

The academy ensures an appropriate filtering system is installed and checked regularly by IT staff. Any issues of concern are raised with a member of the senior leadership team who will deal with the matter appropriately in line with Academy policies. Grace Academy Solihull also utilises in lesson monitoring e.g. Impero.

5.6 Consent

Photographs that include staff and students will be selected carefully. Students' full names will not be used anywhere on the Academy website or other public facing websites, particularly in association with photographs. Written (or verbal – phone call noted on SIMS) permission from parents or carers will be obtained before photographs of students are published on any public facing website. Work can only be published with the permission of the student and parents/carers.

Permission will be obtained from staff in respect of publication of their photographs and original work on any public facing websites or social media accounts.

6. Pupils

6.1 Access to ICT facilities

ICT facilities are available to pupils under the following circumstances:

Computers and equipment in the academy's ICT suite are available to pupils only under the supervision of staff

Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff

Pupils will be provided with an account linked to the academy's GSuite, which they can access from any device by using the Google platform

Sixth-form pupils can use the computers in Post 16 and their academy provision of devices, Chromebook/iPad independently for educational purposes only

Where pupils are required to learn away from the academy, an appropriate Distance Learning environment will be provided, and pupils are expected to follow the same etiquette and protocols as in a classroom environment.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the academy has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under academy rules or legislation.

The academy can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the academy's rules.

This is carried out under Safeguarding and may be recorded accordingly.

6.3 Effective use of the internet

Use of internet derived materials used by staff and students must comply with copyright law and not involve plagiarism. Online plagiarism programmes will be used to sample and moderate work. Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy throughout the curriculum. Students will be taught across the curriculum to acknowledge the source of information and to respect copyright when using internet material in their own work.

6.4 Unacceptable use of ICT and the internet outside of academy

The academy will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on academy premises):

Using ICT or the internet to breach intellectual property rights or copyright

Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

Breaching the academy's policies or procedures

Any illegal conduct, or statements which are deemed to be advocating illegal activity

Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

Activity which defames or disparages the academy, or risks bringing the academy into disrepute

Sharing confidential information about the academy, other pupils, or other members of the academy community

Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities

Causing intentional damage to ICT facilities or materials

Taking photographs or videos of other pupils, staff or visitors of the Academy

Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

Using inappropriate or offensive language

The academy sanctions are outlined in the Student Behaviour Policy.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the academy's ICT facilities as a matter of course.

However, parents working for, or with, the academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the academy's facilities at the principal's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the academy online

We believe it is important to model for pupils and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the academy through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

7.3 Consent

The academy does not require consent to carry out its public duties. The academy may ask for consent in a number of ways where under GDPR it is the only lawful basis. This includes but is not limited to:

Permission obtained from parents in respect of publication of pupil photographs and original work on any public facing websites or social media accounts.

8. Data security

The academy takes steps to protect the security of its computing resources, data and user accounts. However, the academy cannot guarantee security. Staff, pupils, parents and others who use the academy's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

The protocols ensure passwords are changed every 60 days and AD and Google password are synchronised for ease and convenience of a single sign on.

8.2 Software updates, firewalls, and anti-virus software

All of the academy's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the academy's ICT facilities.

Any personal devices using the academy's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the academy's Data Protection Policy.

The academy Data Protection Policy can be found on the academy website.

8.4 Access to facilities and materials

All users of the academy's ICT facilities will have clearly defined access rights to academy systems, files and devices.

These access rights are managed by ICT Lead.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert ICT Support team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The academy ICT team ensures that its devices and systems have an appropriate level of encryption including hard drives – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

Academy staff may only use personal devices (including computers and USB drives) to access academy data, work remotely, or take personal data (such as pupil information) out of academy if they have been specifically authorised to do so by the principal. To minimise this risk the academy has enabled google drives for secure data transfer.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Support team.

9. Internet access

The academy wireless internet connection is secured.

Wi-Fi is monitored using the same system as wired connections

Staff and pupils have separate filtering access. Filtering is appropriate to the user.

BYOD Pupil connections are limited to a small number of educational uses. E.g. Google, SMHW.

Not all filtering is perfect, and we encourage any potential issue to be raised immediately with the IT lead

9.1 Pupils

Wi-Fi is available throughout the building

Pupils have to authenticate to the network using their AD domain username and password any BYOD.

BYOD use is limited to the canteen/street/hall.

9.2 Parents and visitors

Parents and visitors to the academy will not be permitted to use the academy's Wi-Fi unless specific authorisation is granted by the principal.

The principal will only grant authorisation if:

Parents are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA)

Visitors need to access the academy's WIFI in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Parents and Visitors are subject to the Acceptable Use Statement (Appendix 4) and this policy.

Staff must not give the WIFI password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The principal and ICT Lead/ICT manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the academy.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

11. Emerging Technologies

Appropriately planned pilot programmes will be carried out for emerging technologies that may be of educational or administrative benefit. These programmes will be evaluated against student engagement, positive impact on learning and/or increased productivity before they are introduced across the Academies. In circumstances when new technology or technological ideas are considered, the impact will be clearly evaluated.

12. Training

12.1 Staff and Governors

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up

- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The Designated Safeguarding Leads (DSLs) and Deputy Designated Safeguarding Leads (DDSLs) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

As part of Level One safeguarding training, staff should receive training on the basics of E-Safety. Staff receive relevant GDPR and Teaching standards/code of conduct guidance at the start and end of the academic year. Staff receive regular updates in the use of ICT in the classroom and through CPD sessions and professionalism at all times. Governors will be notified of opportunities to complete training.

Incidents are logged through CPOMs.

12.2 Pupils

Students will be informed that network and Internet use will be monitored. A programme of training in e-Safety has been developed in the Academy with regard to the Safeguarding Policy. This is embedded in the curriculum, PSHE and Ethos.

13. Online Safety

The academy has robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

The academy delivers an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

Clear mechanisms are established to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

The academy's approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools.

13.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the principal to account for its implementation.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the DSL.

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

13.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

13.3 The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Leads [and deputy/deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents.

Managing all online safety issues and incidents in line with the school child protection policy.

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the principal and/or governing board

This list is not intended to be exhaustive.

13.4 The ICT manager

The ICT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are

kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

Installing anti-virus and anti-spyware software

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

Conducting a full security check and monitoring the school's ICT systems on a [weekly/fortnightly/monthly] basis.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

13.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

13.6 Parents

Parents are expected to:

Notify a member of staff or the principal of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

13.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

13.8 Educating Pupils

In **Key Stage 3**, pupils will be taught to:

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.

How to report a range of concerns.

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

13.9 Educating Parents and Carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website]. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the principal.

13.10 Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see also the Student Behaviour Policy).

Complaints of internet misuse will be dealt with by the academy in line with the Student Behaviour Policy. Any complaint about staff misuse must be referred to the Principal. Issues relating to child protection must be dealt with in accordance with Academy child protection procedures and the Child Protection Policy.

This policy will be reviewed every year by the ICT Lead or an appropriate member of the academy leadership team. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Related policies

This policy should be read alongside the academy's other policies, including:

- Safeguarding and Promoting Student Welfare Policy
- Student Behaviour Policy
- Staff Code of Conduct and Discipline Policy
- Data Protection Policy

Appendix 1: Facebook and social media guidelines for staff

Don't accept friend requests from pupils on social media

10 rules for academy staff on Facebook usage:

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional. Profile pictures are never private on Facebook and, therefore, due consideration should be taken to ensure that these are appropriate for pupils and colleagues to see.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils.

6. Don't use social media sites during academy hours.
7. Don't make comments about your job, your colleagues, our academy or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at an academy event).
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same WIFI connection (such as parents or pupils).

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.

Don't forget to check your **old posts and photos** and ensure that all content associated with your profile is appropriate.

The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public,** including your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if…

A pupil adds you on social media

Never accept a friend request from a student on social media.

In the first instance, ignore and delete the request. Block the pupil from viewing your profile.

Check your privacy settings again, and consider changing your display name or profile picture.

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.

Notify the senior leadership team or the principal about what's happening.

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the academy.
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in.

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way.

Save evidence of any abuse by taking screenshots and recording the time and date it occurred.

Report the material to Facebook or the relevant social network and ask them to remove it.

If the perpetrator is a current pupil or staff member, the academy's mediation and disciplinary procedures will be implemented to deal with online incidents.

If the perpetrator is a parent or other external adult, a senior member of staff will invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, the targeted staff member or a senior leader should consider contacting the police.

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our academy. The academy uses the following channels: ● Our official Facebook, Twitter and Instagram pages ● Email/text groups for parents (for academy announcements and information) ● Parentmail ● Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the academy via official communication channels, or using private/independent channels to talk about the academy, I will: ● Be respectful towards members of staff, and the academy, at all times. ● Be respectful of other parents/carers and children. ● Direct any complaints or concerns through the academy's official channels, so they can be dealt with in line with the academy's complaints procedure. I will not: ● Use private groups, the academy's social media pages, or personal social media to complain about or criticise members of staff. This is not constructive, and the academy can't improve or address issues if they aren't raised in an appropriate way. ● Use private groups, the academy's social media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident. ● Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers. I will use the school office as the first point of contact if I need to get in touch with their child during the school day, and will endeavour to not try to contact my child on his/her personal mobile during the school day.	
Signed:	**Date:**

Appendix 3: Acceptable use agreement pupils

Acceptable use of the academy's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the academy's ICT facilities and accessing the internet in academy, I will not: ● Use them for a non-educational purpose. ● Access, or attempt to access other user's areas or files. ● Cause damage or interfere with ICT equipment e.g. repair, swap, replace… ● Use facilities without a teacher being present, or without a teacher's permission. ● Use facilities to break academy rules. ● Access any inappropriate websites such as access to pornographic, racist or offensive material. ● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity). ● Use chat rooms, gaming sites or sites of financial benefit. ● Photograph or video other pupils, staff or visitors. ● Abuse the copyright or intellectual property rights of others or plagiarise material. ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher. ● Use any inappropriate language when communicating online, including in emails. ● Give out personal details or knowingly fail to follow E-Safety advice. ● Share my password with others or log in to the academy's network using someone else's details. ● Bully other people. I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the academy's ICT systems and internet responsibly. I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in academy when I do them. I will adhere to the guidance in the ICT policy.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in academy, and will make sure my child understands these. I will adhere to the guidance in the ICT policy.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the academy's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the academy's ICT facilities and accessing the internet in academy, or outside of the academy on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material). ● Use ICT facilities in any way which could harm the academy's reputation. ● Access social networking sites or chat rooms. ● Use any improper language when communicating online, including in emails or other messaging services. ● Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network. ● Share my password with others or log in to the academy's network using someone else's details. ● Share confidential information about the academy, its pupils or staff, or other members of the community. ● Access, modify or share data I'm not authorised to access, modify or share. ● Promote private businesses, unless that business is directly related to the academy.	
I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy. I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the academy's ICT systems and internet responsibly and ensure that pupils in my care do so too. I will adhere to the guidance in the ICT policy.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5 - Use of Mobile Phones and BYOD

1. Introduction and aims

At Grace Academy Solihull we recognise that mobile phones and BYOD, including smart phones, are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

Our policy aims to:

- Promote, and set an example for, safe and responsible phone use.
- Set clear guidelines for the use of mobile phones for pupils, staff, parents and volunteers.
- Support the academy's other policies, especially those related to child protection and behaviour

2. Roles and responsibilities

2.1 Staff

All staff (including teachers, support staff, and supply staff) are responsible for enforcing this policy.
Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.
The ICT Lead or principal is responsible for monitoring the policy every 2 years, reviewing it, and holding staff and pupils accountable for its implementation.

3. Use of mobile phones by staff

3.1 Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while undertaking loco parentis. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room).
There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time. For instance:

- For emergency contact by their child, or their child's school.
- In the case of acutely ill dependents or family members.

The principal will decide on a case-by-basis whether to allow for special arrangements.
If special arrangements are not deemed necessary, school staff can use the school office number 0121 329 4600 as a point of emergency contact.

3.2 Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information.

The data protection policy can be found on the academy website.

3.3 Safeguarding

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils.
Staff must not use their mobile phones to take photographs or recordings of pupils, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

3.4 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations.
- Supervising off-site trips.
- Supervising residential visits.

School Trip phones are available for school trips, but it may be necessary for staff to use their mobile phone and professional judgement should be used in these circumstances.
In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct.
- Not use their phones to take photographs or recordings of pupils, or anything else which could identify a pupil.
- Refrain from using their phones to contact parents. If necessary, contact must be made via the school office.

3.5 Sanctions

Staff that fail to adhere to this policy may face disciplinary action.
See the academy staff disciplinary policy for more information.

4. Use of mobile phones by pupils

Pupils are encouraged to take a responsible role in the use of technology, including mobile phones.

- Pupils are allowed to bring a mobile to school to facilitate, for instance:
    - Travelling to school by themselves
    - Young carers' ability to be contactable
- Pupils are allowed to use their phones at break and lunch in the canteen/street/hall. Pupils may be able to use them at other times at the direction of the teacher for classroom activities/trips and visits/educational activities only.

Access to the system is restricted.

Pupils must adhere to the academy's acceptable use agreement for mobile phone use (see appendix 1).

4.1 Sanctions

- Phones may be confiscated from pupils where appropriate to ensure that, for example, safeguarding practices are adhered to or in line with the Student Behaviour Policy (schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006).

- In the case of confiscation of a pupil's personal device, the pupil must attend a detention with their tutor before collecting from the academy main reception. In safeguarding related incidents, a member of the safeguarding team will discuss the individual circumstances and the related outcome. This will be recorded in line with the academy's safeguarding practices (i.e. using CPOMS).

Staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation. The DfE guidance allows a member of staff to search a pupil's phone if you have reason to believe the phone contains pornographic images, or if it is being/has been used to commit an offence or cause personal injury. Staff must be acting in response to a safeguarding referral in these cases and a member of the safeguarding team will undertake a search if required. Staff will attempt to gain consent from the child, if deemed responsible, or the parent prior to a search of a phone being undertaken.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate. Such conduct includes, but is not limited to:

- Sexting
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation.

5. Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This includes:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child.
- Using any photographs or recordings for personal use only, and not posting on social media without consent.
- Not using phones in lessons, or when working with pupils.

Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal mobile during the school day.

6. Loss, theft or damage

Pupils bringing phones to school must ensure that phones are appropriately labelled and are stored securely when not in use.

Pupils must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone's functions. Staff must also secure their personal phones, as well as any work phone provided to them. Failure by staff to do so could result in data breaches.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Parents are made aware by:

- Disclaimers in the acceptable use
- Disclaimer in home-school agreement
- Disclaimers on trips and visits

Confiscated phones will be stored in the Main Reception.
The academy will note the condition of the phone when confiscated and record this in a log.

Lost phones should be returned to Main Reception. The academy will then attempt to contact the owner.