



Grace Academy Solihull

Digital Policy

(Incorporating ICT and Internet use)

Policy Reference:	GA-P113
Version:	V15
Status	Operational
Authors	M Davies-Friend
Applicable to	Staff, Students, Parents, Visitors & Governors
Checked by	Board
Valid From	March 2020
Review Date	March 2022



Table of Contents

1. Introduction and aims	2
2. Relevant legislation and guidance	2
3. Definitions	2
4. Unacceptable use	3
5. Staff (including governors, volunteers, and contractors)	4
6. Pupils	7
7. Parents	9
8. Data security	9
9. Internet access	10
10. Monitoring and review	11
11. Emerging Technologies	11
12. Training	11
13. E-safety Concerns	12
14. Related policies	12
Appendix 1: Facebook and social media guidelines for staff	13
Appendix 2: Acceptable use of the internet: agreement for parents and carers	15
Appendix 3: Acceptable use agreement for older pupils.....	16
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors	17
Appendix 5 - Use of Mobile Phones and BYOD.....	18
1. Introduction and aims	18
2. Roles and responsibilities.....	18
3. Use of mobile phones by staff	18
4. Use of mobile phones by pupils	19
5. Use of mobile phones by parents, volunteers and visitors.....	20
6. Loss, theft or damage.....	20



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 2019](#)
- [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 social media platforms.

“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 policies on behaviour staff code of conduct.

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

Copies of the Behaviour Policy 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 help@gas-ict.on.spiceworks.com

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, but not exhaustive, include 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).

5.3 Remote access

We allow staff to access the academy's ICT facilities and materials remotely.

Remote access to the academy system will be provided:

The remote access is provided through Smoothwall VPN

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 absent from the Academy your web-based access may be frozen. Should there be any cause for concern the Principal may at their discretion instruct the IT Services Manager to freeze your access 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. For example:



“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 Google Workspace, which they can access from any device ”

“Sixth-form pupils can use the computers in Post 16 and their academy provision of devices i.e Chromebook 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 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 exhaustive of:

Permission will be 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 IT Services Manager.

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 at the end of each working day.

8.5 Encryption

The academy ensures that its devices and systems have an appropriate level of encryption.

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 using 802.1x protocol.

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 connections are limited to a small number of appropriate websites.

Not all filtering is perfect, and we encourage any potential issue be raised with a member of the safeguarding team as well as the assistant leadership team.



13. E-safety Concerns

Complaints of internet misuse will be dealt with by the Academy consequences systems. 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.

14. Related policies

This policy should be read alongside the academy's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff code of conduct and discipline policy
- Data protection



Appendix 1: Facebook and social media guidelines for staff

Do not accept friend requests from pupils on social media

10 rules for academy staff on Facebook

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
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 a 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) - only when using the BYOD connection

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**

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**

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

What do to if...

A pupil adds you 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, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should 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, you 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/carers:	
Name of child:	
<p>Online channels are an important way for parents/carers to communicate with, or about, our academy. The academy uses the following channels:</p> <ul style="list-style-type: none">• Our official Facebook page• Email/text groups for parents (for academy announcements and information) Parentmail• Our virtual learning platform <p>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).</p>	
<p>When communicating with the academy via official communication channels, or using private/independent channels to talk about the academy, I will:</p> <ul style="list-style-type: none">• 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 <p>I will not:</p> <ul style="list-style-type: none">• Use private groups, the academy's Facebook page, 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 Facebook page, 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	
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:	
<p>When using the academy's ICT facilities and accessing the internet in academy, I will not:</p> <ul style="list-style-type: none"> • Use them for a non-educational purpose • Access, or attempt to access other user's user areas or files • Cause damage or interfere with ICT equipment e.g. repair, swap, replace... • Use them without a teacher being present, or without a teacher's permission • Use them 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 and will attempt 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 <p>I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems.</p> <p>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.</p> <p>I will always use the academy's ICT systems and internet responsibly.</p> <p>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.</p> <p>I will adhere to the guidance in the ICT policy.</p>	
Signed (pupil):	Date:
<p>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.</p> <p>I will adhere to the guidance in the ICT policy.</p>	
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 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 them 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 school'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 headteacher 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, their work, 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. The majority of staff have access to an iPad.

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, their work, 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, For instance
 - Travelling to school by themselves
 - Young carers who need 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? (Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006)
- If they are confiscated, 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 will discuss the individual circumstances and the related outcome. This will be recorded on the academy safeguarding system e.g. 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 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 means:

- 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 recorded in a log.

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



ADDENDUM COVID-19

Section referred in Safeguarding Addendum – COVID 19

Online safety

It is likely that children will be using the internet and engaging with social media far more during this time. Our staff are aware of the signs of cyberbullying and other online risks and our filtering and monitoring software remains in use during this time to safeguard and support children. Our staff will follow the process for online safety set out in our Child Protection Policy.

Staff who interact with children online will continue to look out for signs a child may be at risk. If a staff member is concerned about a child, that staff member will follow the approach set out in this addendum and report that concern to the DSL or to a deputy DSL.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, tablets, text messages, emails, instant messages, websites, social media such as Facebook, Twitter, Instagram, chat-rooms, forums, blogs, apps such as Whatsapp, gaming sites, digital cameras, videos, web-cams and other hand-held devices.

Adults should not share any personal information with pupils, and they should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. They should ensure that all communications are transparent and avoid any communication that could be interpreted as 'grooming behaviour'.

Adults must not give their personal contact details such as home/mobile phone number; home or personal e-mail address or social networking details to pupils unless the need to do so is agreed in writing with senior leadership. If, for example, a pupil attempts to locate an adult's personal contact details and attempts to contact or correspond with them, the adult should not respond and must report the matter to their manager.