

# Divide by Staff + Kids

## ARLINGTON PUBLIC SCHOOLS 45 Technology

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

How?

How much testing per grade?

WHAT?

How much training?

What does this mean?

(Students required to access?)

for students?

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

*This applies to all users - not just staff - see next page*

**ARLINGTON PUBLIC SCHOOLS**

**45 Technology**

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

*all about  
staff -  
need to separate  
problems of staff  
from ? student  
work -*

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

**ARLINGTON PUBLIC SCHOOLS**  
**45 Technology**

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

**ARLINGTON PUBLIC SCHOOLS**  
**45 Technology**

---

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

but not here?

here?

↳ employees? contractors

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

who?  
what about replacement of student devices?



ARLINGTON PUBLIC SCHOOLS  
45 Technology

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

Robust & flexibility  
What does that mean?

Training for teachers - esp. using tech meaningfully in classroom

original all in cloud

50% all

present - suite of platforms - BB/GC - to connect - for ex. - teachers start year want to train & implement

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

Can kids  
can have  
laptops up to  
replace up to  
times?  
disciplinary  
could be  
in school

ITC

To support  
but no action  
of this role  
in technology  
assistance.

replacement -  
computers  
repair?  
loss -  
What is requiring  
a notary to  
get a replacement  
computer - Should  
all schools  
require the  
same?

does this apply  
to students or parents?

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, **employees** should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). **Employees or contractors** shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. **Staff members** accessing the APS system are responsible for

mentoring  
**employees**  
in one place &  
**employees or contractors**  
in another place limits the first usage to not include contractors.

How are staff members different from employees?

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

**ARLINGTON PUBLIC SCHOOLS**  
**45 Technology**

---

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

*as an instructional tool to enhance the curriculum and learning experience*

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

ARLINGTON PUBLIC SCHOOLS

45 Technology

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

*Are there specific people or place where staff members can go if they have questions or help to understand the applicable regulations? maybe put that, perhaps information here.*

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

~~Q~~ Answer : why ... the iPad?  
Suggestions: why

- opt-out
- tech-free school
- moment app (quantifier)

### Concerns

- Blue Light
- Attention Span
- Distractability
- Sensory Deprivation
- Displacing other Developmental

- Lack of Empathy (Robot-like kids)
  - Imagination
- Technologies

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

*hacking  
& cheating  
occurs*

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for



**ARLINGTON PUBLIC SCHOOLS**  
**45 Technology**

---

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools → Not in Elementary
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

} This has not happened

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools *(not in elementary school)*
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology *and parents*
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

time well spent  
app.

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

bypassing  
security

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.



The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

*What does this mean?  
- How measured?*

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

*spell out part of student's FOIA ed records*

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

What is "flexibility"? Does this mean  
the ability to use or not use the technology.

ARLINGTON PUBLIC SCHOOLS  
45 Technology

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

APS need  
to more  
clearly  
articulate  
what parts  
of "the"  
mission  
the particular  
type of  
technology  
successfully  
supports

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

Why just  
staff?  
Students  
need access  
to their  
assignments

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

Staff?

Why only

and safety

Students and parents

Canvas, google apps, etc.

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

*why only staff, and digital assets*

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.



The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

flexibility  
Should not  
mean there can  
be a huge  
variation in  
how tech is  
used  
from class to  
class, school to  
school

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.

ARLINGTON PUBLIC SCHOOLS  
45 Technology

The Arlington Public Schools provides a robust and comprehensive data network to support administrative and instructional computing needs of staff and students and assist staff in collecting, processing, and communicating information in an efficient and cost effective manner. In addition, the Arlington Public Schools recognizes the need to manage technological change and establishes procedures and collaborative processes that

*Why?  
This is expensive and not necessarily beneficial. May be harmful. Can be spent other ways.*

- maximize the use of technology to support the mission of The Arlington Public Schools
- provide a robust computing environment allowing students and staff flexibility in accessing data, applications and computing resources
- provide training as required to enable staff to effectively utilize technology
- ensure the security, integrity and privacy of information
- facilitate the integration of applications to eliminate duplication of effort
- adhere to all copyright laws and vendor licensing agreements for products used, and
- when specifically approved, maximize productivity by providing staff remote access to the APS network, applications, and computing resources to complete work at times other than during normal work hours from multiple locations including from their homes.

*Technology should be a tool to reach a goal. Not a mandate*

Access to information contained within the APS internal network and access to global electronic information resources on the Internet are provided by APS to assist employees in effectively performing their work-related functions. Remote access to these services will be provided to staff only upon completion of an approval process included in Policy Implementation Procedure 45-1.6 Technology - Remote Access. A regular, recurring audit process will protect the integrity of APS data and computing resources. Employees are to use APS Internet resources as they would any other type of official APS communications tool.

All data, e-mail, and other types of transmissions composed, transmitted, or retrieved via the Internet or the APS network are considered to be part of the official records of APS and, as such, are subject to disclosure to law enforcement officials, other third parties, and Freedom of Information Act (FOIA) requests. Consequently, employees should ensure that information contained in e-mail messages and other electronic communications are accurate, appropriate, ethical, and lawful. Numerous federal, state and local statutory and regulatory restrictions govern access to information stored within the APS information network (including PCs, LANs, Servers and any type of information or data repository or storage device maintained for/by APS). Employees or contractors shall be allowed access to a system only when they are in full compliance with legal requirements. All information available through any portion of the APS information network or automated systems is protected by policy and in many cases by law and regulation. The information is also subject to all laws and regulations related to the confidentiality of student data and staff personnel records and files and should be protected accordingly. Staff members accessing the APS system are responsible for

---

familiarizing themselves with applicable regulations and for treating all APS information appropriately.

It is the responsibility of staff members who are issued technology equipment to take reasonable precautions to protect the equipment from damage. Staff assumes financial responsibility for repair or replacement of equipment damaged due to negligence or neglect.

Anyone found to have engaged in illegal, unauthorized or unethical practices related to this policy will be subject to disciplinary action that could result in termination of system access, termination of employment and/or criminal prosecution.